

Release Notes for Cisco IOS Release 12.1E on the Catalyst 6500 and Cisco 7600 Supervisor Engine and MSFC

March 4, 2008

Note

- This publication applies to these platforms:
  - CAT6000-SUP2/MSFC2
  - 7600-SUP2/MSFC2
  - CAT6000-SUP1/MSFC2 (not supported in Release 12.2(27b)E2 and later releases)
  - CAT6000-SUP1/MSFC1 (not supported in Release 12.2(27b)E2 and later releases)
- This publication is for Cisco IOS Release 12.1E on both the supervisor engine and the MSFC. If you are running the Catalyst operating system on the supervisor engine and Cisco IOS software only on the MSFC, refer to the *Release Notes for MSFC* publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_2309.htm

In these release notes, the term "MSFC" refers to either an MSFC2 or an MSFC1, except when specifically differentiated.

The term "Catalyst 6500 series switches" includes both Catalyst 6500 series and Catalyst 6000 series switches except where specifically differentiated.

The most current release notes for 12.1E on the Catalyst 6500 series switches and Cisco 7600 Series Routers are available on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/ol_2310.htm

Caution

Cisco IOS running on the supervisor engine and the MSFC supports redundant configurations where the supervisor engines and MSFC routers are identical. If they are not identical, one will boot first and become active and hold the other supervisor engine and MSFC in a reset condition.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 1999–2007 Cisco Systems, Inc. All rights reserved.

Contents

This publication consists of these sections:

- Chronological List of Releases, page 2
- Early Deployment Releases, page 5
- Memory Requirements and Recommendations, page 6
- Supported Hardware, page 8
- Unsupported Hardware, page 28
- Feature Sets, page 29
- Image Names and Sizes, page 51
- New Features, page 51
- Features Not Supported, page 109
- Limitations and Restrictions, page 110
- Caveats, page 119
- Troubleshooting, page 320
- System Software Upgrade Instructions, page 323
- Converting from Catalyst Software, page 323
- Documentation Updates, page 323
- Related Documentation, page 324
- Notices, page 327
- Obtaining Documentation and Submitting a Service Request, page 329

Chronological List of Releases

- 04 Mar 2008—Release 12.1(27b)E4
- 17 Aug 2007—Release 12.1(26)E9
- 10 Aug 2007—Release 12.1(27b)E3
- 12 Jun 2007—Release 12.1(27b)E2
- 22 Jan 2007—Release 12.1(26)E8
- 13 Oct 2006—Release 12.1(27b)E1
- 08 Jun 2006—Release 12.1(26)E7
- 02 Mar 2006—Release 12.1(27b)E
- 06 Feb 2006—Release 12.1(26)E6
- 05 Jan 2006—Release 12.1(26)E5
- 20 Oct 2005—Release 12.1(26)E4
- 09 Sep 2005—Release 12.1(13)E17
- 09 Sep 2005—Release 12.1(8b)E20
- 29 Aug 2005—Release 12.1(23)E4

- 22 Aug 2005—Release 12.1(26)E3
- 30 June 2005—Release 12.1(26)E2
- 12 May 2005—Release 12.1(20)E6
- 10 May 2005—Release 12.1(13)E16
- 09 May 2005—Release 12.1(8b)E19
- 05 May 2005—Release 12.1(23)E3
- 05 May 2005—Release 12.1(22)E6
- 28 Mar 2005—Release 12.1(26)E1
- 20 Jan 2005—Release 12.1(22)E5
- 10 Jan 2005—Release 12.1(26)E
- 06 Dec 2004—Release 12.1(22)E4
- 04 Nov 2004—Release 12.1(23)E2
- 14 Oct 2004—Release 12.1(22)E3
- 16 Sep 2004—Release 12.1(23)E1
- 12 Aug 2004—Release 12.1(13)E15
- 29 Jul 2004—Release 12.1(23)E
- 10 Jun 2004—Release 12.1(22)E2
- 20 Apr 2004—Release 12.1(22)E1
- 20 Apr 2004—Release 12.1(20)E3
- 31 Mar 2004—Release 12.1(13)E14
- 22 Mar 2004—Release 12.1(22)E
- 02 Feb 2004—Release 12.1(20)E2
- 19 Jan 2004—Release 12.1(8b)E18
- 19 Jan 2004—Release 12.1(13)E13
- 19 Jan 2004—Release 12.1(11b)E14
- 18 Dec 2003—Release 12.1(8b)E16
- 24 Nov 2003—Release 12.1(13)E12
- 27 Oct 2003—Release 12.1(20)E
- 13 Oct 2003—Release 12.1(13)E11
- 08 Sep 2003—Release 12.1(13)E10
- 06 Aug 2003—Release 12.1(19)E1a
- 30 Jul 2003—Release 12.1(12c)E7
- 23 Jul 2003—Release 12.1(11b)E12
- 22 Jul 2003—Release 12.1(8b)E15
- 14 Jul 2003—Release 12.1(13)E9
- 01 Jul 2003—Release 12.1(19)E1
- 30 Jun 2003—Release 12.1(13)E8
- 23 Jun 2003—Release 12.1(13)E7

- 03 Jun 2003—Release 12.1(19)E
- 28 Apr 2003—Release 12.1(8b)E14
- 21 Apr 2003—Release 12.1(13)E6
- 07 Apr 2003—Release 12.1(13)E5
- 03 Feb 2003—Release 12.1(13)E4
- 2 Jan 2003—Release 12.1(11b)E11
- 30 Dec 2002—Release 12.1(8b)E13
- 26 Dec 2002—Release 12.1(13)E3
- 16 Dec 2002—Release 12.1(14)E
- 11 Nov 2002—Release 12.1(13)E1
- 28 Oct 2002—Release 12.1(8b)E12
- 28 Oct 2002—Release 12.1(12c)E5
- 21 Oct 2002—Release 12.1(12c)E4
- 09 Sep 2002—Release 12.1(13)E
- 26 Aug 2002—Release 12.1(12c)E2
- 26 Aug 2002—Release 12.1(11b)E7
- 05 Aug 2002—Release 12.1(12c)E1
- 3 June 2002—Release 12.1(11b)E4
- 28 May 2002—Release 12.1(8b)E11
- 13 May 2002—Release 12.1(11b)E3
- 22 April 2002—Release 12.1(8b)E10
- 15 April 2002—Release 12.1(11b)E2
- 25 Mar 2002—Release 12.1(11b)E1
- 28 Feb 2002—Release 12.1(11b)E
- 20 Feb 2002—Release 12.1(8b)E9
- 17 Feb 2002—Release 12.1(1)E6
- 15 Feb 2002—Release 12.1(7a)E6
- 15 Feb 2002—Release 12.1(3a)E7
- 14 Feb 2002—Release 12.1(2)E2
- 13 Feb 2002—Release 12.1(5c)E12
- 12 Feb 2002—Release 12.1(6)E8
- 21 Jan 2002—Release 12.1(8b)E8
- 17 Dec 2001—Release 12.1(8b)E7
- 03 Dec 2001—Release 12.1(8b)E6
- 26 Oct 2001—Release 12.1(8a)E5
- 17 Sep 2001—Release 12.1(8a)E4
- 20 Aug 2001—Release 12.1(8a)E3
- 07 Aug 2001—Release 12.1(8a)E2

- 11 Jul 2001—Release 12.1(8a)E
- 14 May 2001—Release 12.1(7a)E1
- 30 Apr 2001—Release 12.1(7)E
- 09 Apr 2001—Release 12.1(6)E1
- 02 Apr 2001—Release 12.1(5c)E10
- 27 Mar 2001—Release 12.1(5c)E9
- 26 Mar 2001—Release 12.1(6)E
- 05 Mar 2001—Release 12.1(5c)E8
- 22 Jan 2001—Release 12.1(5a)E3
- 28 Dec 2000—Release 12.1(5a)E1
- 20 Nov 2000—Release 12.1(4)E1
- 24 Oct 2000—Release 12.1(3a)E4
- 10 Oct 2000—Release 12.1(3a)E3
- 26 Jun 2000—Release 12.1(2)E
- 20 Feb 2000—Release 12.1(1)E2

Note Some earlier versions of Cisco IOS Software Release 12.1E may no longer be available for download on Cisco.com. For more information, see *Product Bulletin No. 2863, Cisco IOS Software Release Simplification*. See also the list of deferred images in the Cisco IOS Upgrade Planner.

Early Deployment Releases

Release 12.1E supports the Catalyst 6500 series switches and Cisco 7600 series routers.

Release 12.1E is an early deployment release based on Release 12.1. All features and functionality in Release 12.1(26) and earlier 12.1E releases are in Release 12.1(26)E6.

For information on earlier releases, refer to these publications on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm

For more information about the Cisco IOS software release process, refer to the Cisco IOS Software Releases: Product Bulletin #537 on Cisco.com at this URL:

http://www.cisco.com/warp/public/cc/pd/iosw/iore/prodlit/537_pp.htm

This publication does not describe features that are available in Release 12.1, Release 12.1 T, or other Release 12.1 early deployment releases.

All caveats resolved in Release 12.1(26) and earlier 12.1E releases are also resolved in Release 12.1(26)E6. For a list of the open caveats that apply to Release 12.1(26)E6, see the "Caveats" section on page 119 and refer to the *Caveats for Cisco IOS Release 12.1* publication:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121relnt/121cavs/121mcavs.htm

For general product information about the Catalyst 6500 series switches, refer to the Catalyst 6500 Series Software Product Bulletin (URL below):

http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/

Memory Requirements and Recommendations

These sections describe memory requirements:

- Supervisor Engine 2, PFC2, and MSFC2 Default and Recommended Configurations, page 6
- Supervisor Engine 2, PFC2, DFCs, and MSFC2 with EIGRP or OSPF, page 6
- Supervisor Engine 2, PFC2, DFCs, and MSFC2 with BGP, page 7
- Supervisor Engine 2 and MSFC2 Upgrades, page 7
- Supervisor Engine 1, PFC, MSFC, and MSFC2 Default and Recommended Configurations, page 8

Supervisor Engine 2, PFC2, and MSFC2 Default and Recommended Configurations

	Default Configuration		Recommendations	
Supervisor Engine Part Number	**DRAM**	**Bootflash**	**DRAM**	**Bootflash**
WS-X6K-S2U-MSFC2:				
MSFC2	256 MB	32[1] MB	256 MB	32[1] MB
Supervisor Engine 2	256 MB	32 MB	256 MB	32 MB
WS-X6K-S2-MSFC2:				
MSFC2	128 MB[2]	32[1] MB	256 MB	32[1] MB
Supervisor Engine 2	128 MB[2]	32 MB[3]	128 MB	32 MB

1. The bootflash size might be 16 MB. Enter the **show version** command to display the "Flash internal SIMM" size. You cannot boot a supervisor engine image stored in the MSFC2 bootflash.
2. For large networks or complex configurations, we recommend upgrading the memory on the MSFC2 prior to loading 12.1(8a)E or later (see the "Supervisor Engine 2 and MSFC2 Upgrades" section on page 7).
3. The sup-bootflash size might be 16 MB. A 16-MB bootflash device is not large enough to store the supervisor engine image on the supervisor engine bootflash. Enter the **remote command switch show version** command to display the "Flash internal SIMM" size and upgrade if necessary.

Supervisor Engine 2, PFC2, DFCs, and MSFC2 with EIGRP or OSPF

	Maximum Number of EIGRP or OSPF Routes per CEF Path	
Memory Configuration	**Variable Length Subnet Masking**	**Fixed Length Subnet Masking**
MSFC2 with 128 MB, Supervisor Engine 2 with 128 MB, DFC with 128 MB	10,000 routes	20,000 routes

Note Install more memory if your configuration exceeds the limits shown.

Supervisor Engine 2, PFC2, DFCs, and MSFC2 with BGP

Memory Configuration	Maximum Number of BGP Routes per CEF Path	
	Variable Length Subnet Masking	Fixed Length Subnet Masking
MSFC2 with 512 MB, Supervisor Engine 2 with 512 MB, DFC with 256 MB	150,000 routes	250,000 routes
MSFC2 with 256 MB, Supervisor Engine 2 with 256 MB, DFC with 128 MB	64,000 routes	150,000 routes
MSFC2 with 128 MB, Supervisor Engine 2 with 128 MB, DFC with 128 MB	32,000 routes	50,000 routes

Note Install more memory if your configuration exceeds the limits shown.

Supervisor Engine 2 and MSFC2 Upgrades

These publications describe Supervisor Engine 2 and MSFC2 upgrades:

- MSFC2 DRAM— Refer to this publication:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_6953.htm
- Supervisor Engine 2 DRAM—Refer to this publication:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12693.htm
- Supervisor Engine 2 Bootflash—Refer to this publication:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12667.htm
- Supervisor Engine 2 ROMMON software release 7.1(1)—Refer to this publication:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_13488.htm
- DFC—Refer to this publication:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12409.htm

Supervisor Engine 1, PFC, MSFC, and MSFC2 Default and Recommended Configurations

These are the required memory configurations for c6sup11 and c6sup12 images:

- MSFC2 on Supervisor Engine 1—These default memory configurations are acceptable for all MSFC2 images:
  - 128-MB synchronous dynamic random-access memory (SDRAM) DIMM
  - 16-MB Flash SIMM or 32-MB Flash SIMM

Note 128 MB is the minimum acceptable MSFC2 DRAM configuration. We recommend 256 MB or 512 MB of DRAM for large networks or complex configurations.

- MSFC1:
  - 128-MB SDRAM DIMM (upgrade from 64 MB if necessary)
  - 16-MB Flash SIMM
- Supervisor Engine 1—These default memory configurations are acceptable:
  - 64-MB SDRAM DIMM
  - 16-MB Flash SIMM

Supported Hardware

Note
- Use the values in the "Power Required" column to determine the exact power requirements for your configuration to ensure that you are within the power budget. Enter the **show power** command to display current system power usage.
- With Supervisor Engine 2, the minimum software version is Release 12.1(8a)E or later.

- Supervisor Engines, page 9
- Distributed Forwarding Card, page 10
- Switch Fabric Modules, page 11
- 10-Gigabit Ethernet Switching Modules, page 11
- Gigabit Interface Converters (GBICs), page 12
- Gigabit Ethernet Switching Modules, page 12
- 10/100/1000 Ethernet Switching Modules, page 14
- Fast Ethernet Switching Modules, page 15
- Ethernet/Fast Ethernet (10/100) Switching Modules, page 15
- Ethernet Switching Module, page 17
- Optical Services Modules, page 17
- FlexWAN Modules, page 21

- FlexWAN Module Port Adapters, page 21
- Service Modules, page 22
- Power Supplies, page 24
- Fan Trays, page 25
- Chassis, page 26

Supervisor Engines

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
Supervisor Engine 2, PFC2, and MSFC2			
Note Memory and ROMMON can be upgraded (see the "Memory Requirements and Recommendations" section on page 6).			
WS-X6K-S2U-MSFC2	3.46 A	Supervisor Engine 2 with ROMMON version 6.1(3) or later, 32-MB bootflash device, 256-MB DRAM, dual-port 1000BASE-X GBIC uplinks, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**, Number of ports: 2 Number of port groups: 1 Port ranges per port group: 1–2 Policy Feature Card 2 (PFC2), and Multilayer Switch Feature Card 2 (MSFC2)	12.1(8a)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2
WS-X6K-S2-MSFC2	3.46 A	Supervisor Engine 2 with ROMMON version 6.1(2) or later, 16-MB bootflash device, 128-MB DRAM, dual-port 1000BASE-X GBIC uplinks, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**, Number of ports: 2 Number of port groups: 1 Port ranges per port group: 1–2 Policy Feature Card 2 (PFC2), and Multilayer Switch Feature Card 2 (MSFC2)	12.1(8a)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
Supervisor Engine 1 with MSFC1 or MSFC2			
Note			
• Not supported in Release 12.2(27b)E2 and later releases. • Memory and ROMMON can be upgraded (see the "Memory Requirements and Recommendations" section on page 6).			
WS-X6K-S1A-MSFC2	2.90 A	Supervisor Engine 1 with ROMMON version 5.2(1) or later, dual-port 1000BASE-X GBIC uplinks, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**, Number of ports: 2 Number of port groups: 1 Port ranges per port group: 1–2 Policy Feature Card (PFC), and Multilayer Switch Feature Card 2 (MSFC2)	12.1(2)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2
WS-X6K-SUP1A-MSFC	3.30 A	Supervisor Engine 1 with ROMMON release 5.2(1) or later, dual-port 1000BASE-X GBIC uplinks, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**, Number of ports: 2 Number of port groups: 1 Port ranges per port group: 1–2 Policy Feature Card (PFC) and Multilayer Switch Feature Card 1 (MSFC1)	12.1(1)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2

Distributed Forwarding Card

Note

- Supported only with Supervisor Engine 2.
- Supported only in 6500-series chassis.
- Requires Switch Fabric Module.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC	2.10 A	Distributed Forwarding Card (DFC) with 128-MB DRAM, for use on fabric-enabled modules	12.1(8a)E

Switch Fabric Modules

Note

- Supported only with Supervisor Engine 2.
- Supported only in Cisco 7600 series chassis and 6500-series chassis. Not supported in 6000-series chassis.
- Not supported in 3-slot chassis.
- Except in 13-slot chassis, WS-X6500-SFM2 and WS-C6500-SFM can be used together to provide redundancy.

Product Number (append with "=" for spares)	**Power Required**	**Product Description**	**Minimum Software Version**
WS-X6500-SFM2	2.79 A	Switch Fabric Module, version 2, to support fabric-enabled modules **Note** Supports all chassis.	12.1(8a)E
WS-C6500-SFM	2.79 A	Switch Fabric Module to support fabric-enabled modules **Note** Does not support 13-slot chassis.	12.1(8a)E

10-Gigabit Ethernet Switching Modules

Note Release 12.1(8a)EX provides support only with Supervisor Engine 2. Later releases provide support with both Supervisor Engine 2 and Supervisor Engine 1 with MSFC2.

Product Number (append with "=" for spares)	**Power Required**	**Product Description**	**Minimum Software Version**
WS-X6502-10GE	1.94 A	1-port 10-Gigabit Ethernet, fabric-enabled, QoS port architecture (Rx/Tx): **1p1q8t/1p2q1t** Number of ports: 1 Number of port groups: 1 Port ranges per port group: 1 port in 1 group	12.1(11b)E
Note The WS-X6502-10GE module does not support ISL encapsulation.			
Optical Interface Module (OIM) for WS-X6502-10GE			
WS-G6488		10GBASE-LR serial 1310 nm long-haul OIM	12.1(11b)E
WS-G6483		10GBASE-ER serial 1550 nm extended-reach OIM	12.1(13)E

Gigabit Interface Converters (GBICs)

Note The support listed in this section applies to all modules that use GBICs, including OSM LAN ports and OSM Gigabit Ethernet WAN ports.

Product ID (append "=" for spares)	Product Description	Minimum Software Version
DWDM-GBIC	Dense wavelength division multiplexing (DWDM) GBIC	12.1(20)E2
CWDM-GBIC	Coarse wave division multiplexing (CWDM) GBIC	12.1(13)E
WS-G5483	1000BASET GBIC	12.1(13)E
WS-G5484	Short wavelength, 1000BASE-SX	12.1(1)E
WS-G5486	Long wavelength/long haul, 1000BASE-LX/LH	12.1(1)E
WS-G5487	Extended distance, 1000BASE-ZX	12.1(1)E

Gigabit Ethernet Switching Modules

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6816-GBIC	5.94 A	16-port Gigabit Ethernet GBIC, fabric-enabled, dual switch fabric interfaces, WS-F6K-DFC-equipped, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Dual switch fabric connections –Fabric Channel #1: Ports 1–8 –Fabric Channel #2: Ports 9–16 Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16 **Note** Supported only with Supervisor Engine 2. Requires Switch Fabric Module. In WS-C6513 chassis, supported only in slots 9 through 13.	12.1(8a)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2
WS-X6516A-GBIC	3.62 A	16-port Gigabit Ethernet GBIC, CEF256 (dCEF256 with DFC), 1-MB per-port packet buffers, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	12.1(19)E1

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6516-GBIC	3.40 A	16-port Gigabit Ethernet GBIC, CEF256 (dCEF256 with DFC), QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	12.1(8a)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2
WS-X6416-GBIC	2.81 A	16-port Gigabit Ethernet GBIC, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	12.1(2)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2
WS-X6416-GE-MT	2.50 A	16-Port Gigabit Ethernet MT-RJ, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	12.1(2)E
WS-X6408A-GBIC	2.00 A	8-port Gigabit Ethernet GBIC QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Number of ports: 8 Number of port groups: 1 Port ranges per port group: 1–8	12.1(1)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2
WS-X6408-GBIC	2.00 A	8-port Gigabit Ethernet GBIC QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 8 Number of port groups: 1 Port ranges per port group: 1–8	12.1(1)E
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E
		With DWDM-GBIC support	12.1(20)E2
WS-X6316-GE-TX	5.15 A	16-port Gigabit Ethernet RJ-45, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	12.1(1)E

10/100/1000 Ethernet Switching Modules

Product Number (append with "=" for spares)	**Power Required**	**Product Description**	**Minimum Software Version**
WS-X6548-GE-TX WS-X6548V-GE-TX	2.98 A 3.40 A	48-port 10/100/1000 Mbps, RJ-45, fabric-enabled (WS-X6548V-GE-TX has WS-F6K-VPWR-GE) QoS port architecture (Rx/Tx): **1q2t/1p2q2t** Number of ports: 48 Number of port groups: 2 Port ranges per port group: 1–24, 25–48 **Note** See the "New Hardware Features in Release 12.1(19)E1" section on page 66 for a list of unsupported features.	12.1(19)E1
WS-X6148-GE-TX WS-X6148V-GE-TX	2.47 A 2.89 A	48-port 10/100/1000 Mbps, RJ-45 (WS-X6148V-GE-TX has WS-F6K-VPWR-GE) QoS port architecture (Rx/Tx): **1q2t/1p2q2t** Number of ports: 48 Number of port groups: 2 Port ranges per port group: 1–24, 25–48 **Note** See the "New Hardware Features in Release 12.1(19)E1" section on page 66 for a list of unsupported features.	12.1(19)E1
WS-X6516-GE-TX	3.45 A	16-port 10/100/1000 Mbps, RJ-45, fabric-enabled, QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	12.1(8a)EX

Fast Ethernet Switching Modules

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6524-100FX-MM	1.90 A	24-port 100FX Ethernet multimode, fabric enabled, QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** Number of ports: 24 Number of port groups: 1 Port ranges per port group: 1–24	12.1(8a)EX
WS-X6324-100FX-SM WS-X6324-100FX-MM	1.52 A 1.52 A	24-port 100FX Ethernet single mode and multimode MT-RJ with 128-KB per-port packet buffers QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24	12.1(2)E
WS-X6224-100FX-MT	1.90 A	24-port 100FX Ethernet Multimode MT-RJ QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24	12.1(1)E

Ethernet/Fast Ethernet (10/100) Switching Modules

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6548-RJ-45	2.90 A	48-port 10/100TX RJ-45, fabric enabled, QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** Number of ports: 48 Number of port groups: 1 Port ranges per port group: 1–48	12.1(8a)E
WS-X6548-RJ-21	2.90 A	48-port 10/100TX RJ-21, fabric enabled, QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** Number of ports: 48 Number of port groups: 1 Port ranges per port group: 1–48	12.1(8a)EX
WS-X6348-RJ-45 WS-X6348-RJ-45V	2.39 A	48-port 10/100TX RJ-45, 128-KB per-port packet buffers, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	12.1(2)E
		With WS-F6K-VPWR support	12.1(13)E

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6348-RJ-21V	2.39 A	48-port 10/100TX RJ-21, 128-KB per-port packet buffers, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	12.1(8a)EX
		With WS-F6K-VPWR support	12.1(13)E
WS-X6248-RJ-45	2.69 A	48-port 10/100TX RJ-45, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	12.1(1)E
WS-X6248A-TEL	2.69 A	48-port 10/100TX RJ-21, 128-KB per-port packet buffers, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	12.1(2)E
WS-X6248-TEL	2.69 A	48-port 10/100TX RJ-21, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	12.1(1)E
WS-X6148-RJ-45 WS-X6148-RJ-45V	2.39 A	48-port 10/100TX RJ-45, 128-KB per-port packet buffers, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	12.1(12c)E1
		With WS-F6K-VPWR support	12.1(13)E
WS-X6148-RJ-21 WS-X6148-RJ-21V	2.39 A	48-port 10/100TX RJ-21, 128-KB per-port packet buffers, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	12.1(12c)E1
		With WS-F6K-VPWR support	12.1(13)E

Ethernet Switching Module

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6024-10FL-MT	1.52 A	24-port 10BASE-FL MT-RJ, QoS port architecture (Rx/Tx): **1q4t/2q2t** Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24	12.1(1)E

Optical Services Modules

- Gigabit Ethernet WAN, page 17
- OC-48 Packet over SONET, page 18
- OC-48 DPT/Packet over SONET, page 18
- OC-12 Packet over SONET, page 18
- OC-3 Packet over SONET, page 19
- OC-48 Channelized, page 19
- OC-12 Channelized, page 20
- CT3/T1 Channelized/Unchannelized, page 20
- OC-12 ATM, page 20

Note

- Optical services modules (OSMs) are supported only with Supervisor Engine 2.
- OSM WAN port numbering starts with 1.
- On OSMs with Layer 2 LAN ports:
  - The LAN ports are numbered starting with 1.
  - The LAN ports are in a single port group.

Gigabit Ethernet WAN

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-4GE-WAN	3.59 A	4-port Gigabit Ethernet WAN (GBIC)	12.1(8a)EX
		With CWDM-GBIC and WS-G5483 GBIC support	12.1(13)E3
OSM-2+4GE-WAN+	5.08 A	4-port Gigabit Ethernet WAN (GBIC) with 2 Layer 2 LAN ports	12.1(13)E3

OC-48 Packet over SONET

Note

- Also has four Layer 2 Gigabit Ethernet GBIC ports, numbered 1 through 4.
- Support for CWDM-GBIC and WS-G5483 GBIC on the Layer 2 ports requires Release 12.1(13)E1 or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-1OC48-POS-SS	4.25 A	1-port OC-48/STM-16 SONET/SDH OSM, SM-SR	12.1(8a)E3
OSM-1OC48-POS-SI		1-port OC-48/STM-16 SONET/SDH OSM, SM-IR	
OSM-1OC48-POS-SL		1-port OC-48/STM-16 SONET/SDH OSM, SM-LR	
OSM-1OC48-POS-SI+	3.90 A	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-IR	12.1(13)E1
OSM-1OC48-POS-SL+		Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-LR	
OSM-1OC48-POS-SS+		Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-SR	

OC-48 DPT/Packet over SONET

Note

- Also has four Layer 2 Gigabit Ethernet GBIC ports, numbered 1 through 4.
- Support for CWDM-GBIC and WS-G5483 GBIC on the Layer 2 ports requires Release 12.1(13)E1 or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-2OC48/1DPT-SS	5.75 A	2-port OC-48 DPT/POS, SM-SR	12.1(12c)E1
OSM-2OC48/1DPT-SI		2-port OC-48 DPT/POS, SM-IR	
OSM-2OC48/1DPT-SL		2-port OC-48 DPT/POS, SM-LR	

OC-12 Packet over SONET

Note

- Also has four Layer 2 Gigabit Ethernet GBIC ports, numbered 1 through 4.
- Support for CWDM-GBIC and WS-G5483 GBIC on the Layer 2 ports requires Release 12.1(13)E1 or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-4OC12-POS-MM	4.78 A	4-port OC-12c/STM-4c POS, MM	12.1(8a)E3
OSM-4OC12-POS-SI		4-port OC-12c/STM-4c POS, SM-IR	
OSM-4OC12-POS-SL		4-port OC-12c/STM-4c POS, SM-LR	
OSM-4OC12-POS-SI+	4.55 A	Enhanced 4-port OC-12c/STM-4c POS, SM-IR	12.1(13)E1
OSM-2OC12-POS-MM	3.36 A	2-port OC-12c/STM-4c POS, MM	12.1(8a)E3
OSM-2OC12-POS-SI		2-port OC-12c/STM-4c POS, SM-IR	
OSM-2OC12-POS-SL		2-port OC-12c/STM-4c POS, SM-LR	
OSM-2OC12-POS-MM+	3.36 A	Enhanced 2-port OC-12c/STM-4c POS, MM	12.1(13)E1
OSM-2OC12-POS-SI+		Enhanced 2-port OC-12c/STM-4c POS, SM-IR	

OC-3 Packet over SONET

Note

- Also has four Layer 2 Gigabit Ethernet GBIC ports, numbered 1 through 4.
- Support for CWDM-GBIC and WS-G5483 GBIC on the Layer 2 ports requires Release 12.1(13)E1 or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-16OC3-POS-MM	5.09 A	16-port OC-3c/STM-1c POS, MM	12.1(8a)E3
OSM-16OC3-POS-SI		16-port OC-3c/STM-1c POS, SM-IR	
OSM-16OC3-POS-SL		16-port OC-3c/STM-1c POS, SM-LR	
OSM-16OC3-POS-SI+	4.80 A	Enhanced 16-port OC-3c/STM-1c POS, SM-IR	12.1(13)E1
OSM-8OC3-POS-MM	3.57 A	8-port OC-3c/STM-1c POS, MM	12.1(8a)E3
OSM-8OC3-POS-SI		8-port OC-3c/STM-1c POS, SM-IR	
OSM-8OC3-POS-SL		8-port OC-3c/STM-1c POS, SM-LR	
OSM-8OC3-POS-SI+	3.57 A	Enhanced 8-port OC-3c/STM-1c POS, SM-IR	12.1(13)E1
OSM-8OC3-POS-SL+		Enhanced 8-port OC-3c/STM-1c POS, SM-LR	
OSM-4OC3-POS-SI	2.44 A	4-port OC-3c/STM-1c POS, SM-IR	12.1(8a)EX
OSM-4OC3-POS-SI+	2.44 A	Enhanced 4-port OC-3c/STM-1c POS, SM-IR	12.1(13)E11

OC-48 Channelized

Note

- Also has four Layer 2 Gigabit Ethernet GBIC ports, numbered 1 through 4.

- Support for CWDM-GBIC and WS-G5483 GBIC on the Layer 2 ports requires Release 12.1(13)E1 or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-1CHOC48/T3-SS	3.75 A	1-port channelized OC-48, SM-SR	12.1(8a)E3
OSM-1CHOC48/T3-SI		1-port channelized OC-48, SM-IR	

OC-12 Channelized

Note

- Also has four Layer 2 Gigabit Ethernet GBIC ports, numbered 1 through 4.
- Support for CWDM-GBIC and WS-G5483 GBIC on the Layer 2 ports requires Release 12.1(13)E1 or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-4CHOC12/T3-MM	4.49 A	4-port channelized OC-12, SM-SR	12.1(8a)E3
OSM-4CHOC12/T3 -SI		4-port channelized OC-12, SM-IR	
OSM-1CHOC12/T3-SI	4.40 A	1-port channelized OC-12, SM-IR	12.1(12c)E1
OSM-1CHOC12/T1-SI	2.80 A	1-port channelized OC-12, SM-IR	12.1(13)E3

CT3/T1 Channelized/Unchannelized

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-12CT3/T1	2.80 A	12-port channelized/unchannelized CT3/T1. The module has mini-SMB connectors for use with 75-Ohm copper coax cable.	12.1(13)E3

OC-12 ATM

Note

- Also has four Layer 2 Gigabit Ethernet GBIC ports, numbered 1 through 4.
- Support for CWDM-GBIC and WS-G5483 GBIC on the Layer 2 ports requires Release 12.1(13)E1 or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-2OC12-ATM-MM	3.62 A	2-port OC-12/STM-4 ATM OSM, MM	12.1(8b)EX2
OSM-2OC12-ATM-SI		2-port OC-12/STM-4 ATM OSM, SM-IR	
OSM-2OC12-ATM-MM+	4.00 A	Enhanced 2-port OC-12/STM-4 ATM OSM, MM	12.1(12c)E1
OSM-2OC12-ATM-SI+		Enhanced 2-port OC-12/STM-4 ATM OSM, SM-IR	

FlexWAN Modules

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6182-2PA	2.38A	FlexWAN Module	12.1(5a)E1

FlexWAN Module Port Adapters

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
PA-POS-OC3MM PA-POS-OC3SMI PA-POS-OC3SML	Packet over SONET (OC-3)	12.1(1)E
PA-A3-OC3MM PA-A3-OC3SMI PA-A3-T3 PA-A3-OC3SML PA-A3-E3	ATM with traffic shaping **Note** These port adapters do not support LANE when installed in the FlexWAN module.	12.1(1)E
PA-A3-8T1IMA PA-A3-8E1IMA	ATM with traffic shaping **Note** These port adapters do not support LANE when installed in the FlexWAN module.	12.1(12c)E2
PA-T3 PA-T3+ PA-2T3 PA-2T3+ PA-E3 PA-2E3 PA-MC-T3 PA-MC-E3	T3/E3 (clear-channel and channelized)	12.1(1)E
PA-MC-2T3+	T3/E3 (clear-channel and channelized)	12.1(2)E

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
PA-4T+ PA-8T-V35 PA-8T-X21 PA-8T-232 PA-MC-2E1/120 PA-MC-8T1 PA-MC-8E1/120	T1/E1	12.1(1)E
PA-MC-2T1 PA-MC-4T1	T1/E1	12.1(8a)E3
PA-MC-8TE1+	Multichannel T1/E1 8PRI **Note** This port adapter does not support ISDN PRI when installed in the FlexWAN module.	12.1(12c)E1
PA-4E1G/75 PA-4E1G/120	T1/E1	12.1(19)E
PA-H PA-2H	HSSI	12.1(1)E
PA-MC-STM-1	Multichannel STM-1	12.1(7)E

Service Modules

- Communication Media Module (CMM), page 22
- Firewall Services Module, page 23
- Intrusion Detection System Modules (IDSMs), page 23
- Network Analysis Modules (NAMs), page 23
- Content Switching Module (CSM), page 24
- Content Services Gateway (CSG) Module, page 24
- Secure Sockets Layer (SSL) Services Module, page 24

Communication Media Module (CMM)

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-CMM	6.00 A	Communication Media Module	12.1(13)E
Communication Media Module Port Adapters			
WS-SVC-CMM-6E1		6-Port E1 Interface Port Adapter	
WS-SVC-CMM-6T1		6-Port T1 Interface Port Adapter	
WS-SVC-CMM-ACT		Adhoc Conferencing and Transcoding Port Adapter	
WS-SVC-CMM-24FXS		24-Port FXS Interface Port Adapter	

Firewall Services Module

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-FWM-1-K9	4.09 A	Fabric-enabled Firewall Services Module	12.1(13)E

Intrusion Detection System Modules (IDSMs)

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6381-IDS	1.31 A	Intrusion Detection System Module **Note** 12.1(8a)EX releases provide support only with Supervisor Engine 2.	12.1(8a)EX
WS-SVC-IDS2-BUN-K9	2.50 A	Fabric-enabled Intrusion Detection System Module 2	
		With Supervisor Engine 2	12.1(14)E
		With Supervisor Engine 1 and MSFC2	12.1(19)E1

Network Analysis Modules (NAMs)

Note

- 12.1(8a)EX releases provide support for WS-X6380-NAM only with Supervisor Engine 2.
- NAM software release 2.1(2) requires Release 12.1(11b)E or later.
- NAM software release 2.1(2a) requires Release 12.1(13)E or later.

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-NAM-2	3.47 A	Fabric-enabled NAM-2	
		With Supervisor Engine 2	12.1(13)E
		With Supervisor Engine 1 and MSFC2	12.1(19)E1
WS-SVC-NAM-1	2.89 A	Fabric-enabled NAM-1	
		With Supervisor Engine 2	12.1(13)E
		With Supervisor Engine 1 and MSFC2	12.1(19)E1
WS-X6380-NAM	1.31 A	Network Analysis Module with Supervisor Engine 1 and Supervisor Engine 2	12.1(8a)EX

Content Switching Module (CSM)

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6066-SLB-APC	3.00 A	Content Switching Module	
		With Supervisor Engine 2	12.1(8a)E
		With Supervisor Engine 1 and MSFC2	12.1(6)E

Content Services Gateway (CSG) Module

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-CSG-1	3.00 A	Content Services Gateway (CSG) Module	12.1(11b)E

Secure Sockets Layer (SSL) Services Module

Product Number (append with "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-SSL-1	2.94 A	Fabric-enabled Secure Sockets Layer (SSL) Services Module	
		With Supervisor Engine 2	12.1(13)E
		With Supervisor Engine 1 and MSFC2	12.1(19)E1

Power Supplies

- 7603 and 6503 Power Supplies, page 24
- 7606 Power Supplies, page 25
- Other Power Supplies, page 25

7603 and 6503 Power Supplies

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
PWR-1400-AC	1,400 W AC power supply	12.1(20)E
PWR-950-AC	950 W (21.89 A) AC power supply	12.1(8a)E3
PWR-950-DC	950 W (21.89 A) DC power supply	

7606 Power Supplies

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
PWR-1900-AC	1900 W AC power supply	12.1(8a)EX
PWR-1900-DC	1900 W DC power supply	

Other Power Supplies

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
PWR-4000-DC	4000 W DC power supply	12.1(19)E
WS-CAC-3000W	3,000 W AC power supply	12.1(13)E
WS-CAC-4000W	4000 W (95.70 A) AC power supply	12.1(6)E
WS-CAC-2500W	2500 W (55.50 A) AC power supply	
WS-CDC-2500W	2500 W (55.50 A) DC power supply	
WS-CAC-1300W	1300 W (27.46 A) AC power supply	
WS-CDC-1300W	1300 W (27.46 A) DC power supply	
WS-CAC-1000W	1000 W (21.40 A) AC power supply	12.1(1)E

Fan Trays

Note Supervisor Engine 1 and Supervisor Engine 2 do not require a high-capacity fan.

Product Number (append "=" for spares)	Product Description	Minimum Software Version
FAN-MOD-3	Standard-capacity fan tray for WS-C6503 and CISCO7603 chassis	12.1(13)E
FAN-MOD-3HS	High-capacity fan tray for WS-C6503 and CISCO7603 chassis	12.1(20)E
FAN-MOD-6	Standard-capacity fan tray for CISCO7606 chassis	12.1(11b)E
FAN-MOD-6HS	High-capacity fan tray for CISCO7606 chassis	12.1(20)E
FAN-MOD-09	High-capacity fan tray for WS-C6509-NEB-A and CISCO7609 chassis	12.1(13)E3
WS-C6503-E-FAN	High-capacity fan tray for WS-C6503-E chassis	12.1(13)E
WS-C6506-E-FAN	High-capacity fan tray for WS-C6506-E chassis	12.1(1)E
WS-C6509-E-FAN	High-capacity fan tray for WS-C6509-E chassis	12.1(1)E

Product Number (append "=" for spares)	Product Description	Minimum Software Version
WS-C6K-6SLOT-FAN	Standard-capacity fan tray for WS-C6506 chassis	12.1(1)E
WS-C6K-6SLOT-FAN2	High-capacity fan tray for WS-C6506 chassis	12.1(20)E
WS-C6K-9SLOT-FAN	Standard-capacity fan tray for WS-C6509 chassis	12.1(1)E
WS-C6K-9SLOT-FAN2	High-capacity fan tray for WS-C6509 chassis	12.1(20)E
WS-C6509-NEB-FAN=	Standard fan tray for WS-C6509-NEB	12.1(13)E
WS-C6K-13SLT-FAN	Standard-capacity fan tray for WS-C6513 and CISCO7613 chassis	12.1(8a)E
WS-C6K-13SLT-FAN2	High-capacity fan tray for WS-C6513 and CISCO7613 chassis	12.1(20)E

Chassis

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
CISCO7613	Cisco 7613 chassis: • 13 slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2	12.1(13)E4
WS-C6513	Catalyst 6513 chassis: • 13 slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2	12.1(8a)E
CISCO7609	Cisco 7609-NEB chassis • 9 vertical slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2	12.1(13)E3
WS-C6509-NEB-A	Catalyst 6509-NEB chassis • 9 vertical slots • 1024 chassis MAC addresses	12.1(19)E1
WS-C6509-NEB	Catalyst 6509-NEB chassis: • 9 vertical slots • 1024 chassis MAC addresses	12.1(2)E
OSR-7609	Cisco 7609 chassis: • 9 vertical slots • 1024 chassis MAC addresses • Supported only with Supervisor Engine 2	12.1(8a)E3

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
WS-C6509-E	Catalyst 6509 chassis: • 9 slots • 1024 chassis MAC addresses • Requires WS-C6509-E-FAN • Requires 2,500 W or higher power supply	12.1(1)E
WS-C6509	Catalyst 6509 chassis: • 9 slots • 1024 chassis MAC addresses	12.1(1)E
CISCO7606	Cisco 7606 chassis: • 6 slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2	12.1(11b)E
WS-C6506-E	Catalyst 6506 chassis: • 6 slots • 1024 chassis MAC addresses • Requires WS-C6506-E-FAN • Requires 2,500 W or higher power supply	12.1(1)E
WS-C6506	Catalyst 6506 chassis: • 6 slots • 1024 chassis MAC addresses	12.1(1)E
WS-C6503-E	Catalyst 6503 chassis: • 3 slots • 64 chassis MAC addresses • Does not support SFM, SFM2, or WS-F6K-DFC • Requires WS-C6503-E-FAN	12.1(11b)EX 12.1(11b)E7 12.1(12c)E5 12.1(13)E
WS-C6503	Catalyst 6503 chassis: • 3 slots • 64 chassis MAC addresses • Does not support SFM, SFM2, or WS-F6K-DFC	12.1(11b)EX 12.1(11b)E7 12.1(12c)E5 12.1(13)E
CISCO7603	Cisco 7603 chassis: • 3 slots • 64 chassis MAC addresses • Does not support SFM, SFM2, or WS-F6K-DFC	12.1(8a)E3

Product Number (append with "=" for spares)	Product Description	Minimum Software Version
WS-C6009	Catalyst 6009 chassis: • Does not support SFM, SFM2, or WS-F6K-DFC • 9 slots • 1024 chassis MAC addresses	12.1(1)E
WS-C6006	Catalyst 6006 chassis: • Does not support SFM, SFM2, or WS-F6K-DFC • 6 slots • 1024 chassis MAC addresses	12.1(1)E

Unsupported Hardware

The following hardware is not supported:

- In Release 12.2(27b)E2 and later releases, Supervisor Engine 1.
- Supervisor Engine 720
- Supervisor Engine 32
- Distributed Forwarding Card 3 (DFC3A, DFC3B, DFC3BXL)
- WS-X6748-GE-TX 48-port 10/100/1000 RJ-45 Ethernet switching module
- WS-X6748-SFP 48-port Gigabit SFP Ethernet switching module
- WS-X6724-SFP 24-port Gigabit SFP Ethernet switching module
- WS-X6704-10GE 4-port 10-Gigabit XENPAK Ethernet switching module
- WS-X6148A-GE-TX, WS-X6148A-GE-45AF 48-port 10/100/1000 Mbps RJ-45 Ethernet switching module
- WS-X6148A-RJ-45, WS-X6148A-45AF 48-port 10/100TX RJ-45 Ethernet switching module
- WS-X6148-FE-SFP 48-port 100BASE-FX SFP Ethernet switching module
- WS-X6148X2-RJ-45, WS-X6148X2-45AF 96-port 10/100TX RJ-45 RJ-45 Ethernet switching module
- WS-X6196-RJ-21, WS-X6196-21AF 96-port 10/100TX RJ-21 Ethernet switching module
- WS-X6582-2PA Enhanced FlexWAN Module
- These FlexWAN port adapters:
  - PA-A6-OC3MM 1-port ATM OC-3c/STM-1 multimode port adapter, enhanced
  - PA-A6-OC3SMI 1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced
  - PA-A6-OC3SML 1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced
  - PA-A6-T3 1-port ATM DS3 port adapter, enhanced
  - PA-A6-E3 1-port ATM E3 port adapter, enhanced
- WS-SVC-IPSEC1 IPsec Virtual Private Network (VPN) acceleration service module
- WS-SVC-PSD-1 Persistent Storage Device service module

- WS-SVC-MWAM-1 Multi-Processor WAN Application Module
- WS-X6624-FXS, WS-X6608-T1, and WS-X6608-E1 voice modules
- WS-X6101-OC12-MMF and WS-X6101-OC12-SMF ATM LANE modules
- WS-X6302-MSM Multilayer Switch Module

These modules remain powered down if detected and do not affect system behavior.

Feature Sets

These sections describe the feature sets:

- Release 12.1(27b)E4, page 31
- Release 12.1(26)E9, page 34
- Release 12.1(23)E4, page 37
- Release 12.1(22)E6, page 39
- Release 12.1(20)E6, page 42
- Release 12.1(19)E1 and 12.1(19)E1a, page 45
- Release 12.1(14)E, page 45
- Release 12.1(13)E17, page 45
- Release 12.1(12c)E5, page 48
- Release 12.1(11b)E14, page 48
- Release 12.1(8b)E20, page 48
- Release 12.1(7a)E6, page 50
- Release 12.1(6)E8, page 50
- Release 12.1(5c)E12, page 51
- Release 12.1(4)E1, page 51
- Release 12.1(3a)E7, page 51
- Release 12.1(2)E2, page 51
- Release 12.1(1)E6, page 51

Note

- Use of the EGP, BGP4, and IS-IS routing protocols requires the additional purchase of the InterDomain Routing Feature License (FR-IRC6).
- The image names reflect the supervisor engine and MSFC versions. For example:
  - The c6sup22-jsv-mz.121-22.E image is for Supervisor Engine 2 with MSFC2.
  - The c6sup12-jsv-mz.121-22.E image is for Supervisor Engine 1 with MSFC2.
  - The c6sup11-jsv-mz.121-22.E image is for Supervisor Engine 1 with MSFC1.
- Many TFTP implementations cannot transfer 16 MB or larger files. In Release 12.1(8a)E and later releases, system software images for Supervisor Engine 2 are larger than 16 MB. To transfer 16 MB or larger files, you might need to use FTP or rcp. Refer to this online publication for procedures:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt2/fcd203.htm

- The k2 images support the IPsec Network Security feature (configured with the **crypto ipsec** command) in software and SSH access.
- For information about the firewall images, which support Cisco firewall features in software, see the "Configuring Network Security" chapter in the *Software Configuration Guide* at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/secure.htm

Release 12.1(27b)E4

Note For information about the size of Release 12.1(27b)E4 images, see the "Image Names and Sizes in Release 12.1(27b)E4" section.

Feature Set	Image Filename	Orderable Product Number[1]
Enterprise: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2, DECnet Phase IV, and VINES routing • DECnet Phase V and CLNS/OSI routing	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-js-mz.121-27b.E4	S6S22ALV-12127E
	Supports FlexWAN and OSM: c6sup22-jsv-mz.121-27b.E4	S6S22AV-12127E
	Supports SSHv2: c6sup22-jk2s-mz.121-27b.E4	S6S22ALK2-12127E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-jk2sv-mz.121-27b.E4	S6S22AK2-12127E
	Supports FlexWAN, OSM, and firewall: c6sup22-jo3sv-mz.121-27b.E4	S6S22AVH-12127E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-jk2o3sv-mz.121-27b.E4	S6S22ZVH-12127E
	Supervisor Engine 1/MSFC2 images	
	c6sup12-js-mz.121-27b.E1	S6S12A-12127E
	Supports FlexWAN and OSM: c6sup12-jsv-mz.121-27b.E1	S6S12AV-12127E
	Supports SSHv2: c6sup12-jk2s-mz.121-27b.E1	S6S12ALK2-12127E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-jk2sv-mz.121-27b.E	S6S12AK2-12127E
	Supports FlexWAN, OSM, and firewall: c6sup12-jo3sv-mz.121-27b.E1	S6S12AVH-12127E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-jk2o3sv-mz.121-27b.E1	S6S12AK2H-12127E
	Supervisor Engine 1/MSFC images	
	c6sup11-js-mz.121-27b.E1	S6S11A-12127E
	Supports FlexWAN and OSM: c6sup11-jsv-mz.121-27b.E	S6S11AV-12127E
	Supports SSHv2: c6sup11-jk2sv-mz.121-27b.E1	S6S11ALK2-12127E
	Supports FlexWAN, OSM, and SSHv2: c6sup11-jk2sv-mz.121-27b.E	S6S11AK2-12127E

Feature Set	Image Filename	Orderable Product Number[1]
Desktop (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2 and DECnet Phase IV routing	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-27b.E4	S6S22BV-12127E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-27b.E1	S6S12BV-12127E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-27b.E1	S6S11BV-12127E
Service Provider: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP)	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-ps-mz.121-27b.E4	S6S22ZLV-12127E
	Supports FlexWAN and OSM: c6sup22-psv-mz.121-27b.E4	S6S22ZV-12127E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-pk2sv-mz.121-27b.E4	S6S22ZK2-12127E
	Supports FlexWAN, OSM, and firewall: c6sup22-po3sv-mz.121-27b.E4	S6S22ZVH-12127E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-pk2o3sv-mz.121-27b.E4	S6S22ZK2H-12127E
	Supervisor Engine 1/MSFC2 image	
	c6sup12-ps-mz.121-27b.E1	S6S12ZLV-12127E
	Supports FlexWAN and OSM: c6sup12-psv-mz.121-27b.E1	S6S12ZV-12127E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-pk2sv-mz.121-27b.E1	S6S12ZK2-12127E
	Supports FlexWAN, OSM, and firewall: c6sup12-po3sv-mz.121-27b.E1	S6S12ZVH-12127E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-pk2o3sv-mz.121-27b.E	S6S12ZK2H-12127E
	Supervisor Engine 1/MSFC image	
	c6sup11-ps-mz.121-27b.E1	S6S11ZLV-12127E
	Supports FlexWAN and OSM: c6sup11-psv-mz.121-27b.E1	S6S11ZV-12127E
	Supports FlexWAN, OSM, and SSHv2: 6sup11-pk2sv-mz.121-27b.E1	S6S11ZK2-12127E

Feature Set	Image Filename	Orderable Product Number[1]
IP/IPX (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-27b.E4	S6S22DV-12127E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-27b.E1	S6S12DV-12127E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-27b.E1	S6S11DV-12127E
MSFC2 boot loader	c6msfc2-boot-mz.121-27b.E4	N/A
MSFC1 boot loader	c6msfc-boot-mz.121-27b.E1	N/A

1. Installed; append with "=" for spare on shipable media.

Release 12.1(26)E9

Note

- For information about the size of Release 12.1(26)E9 images, see the "Image Names and Sizes in Release 12.1(26)E9" section.
- Release 12.1(26)E and rebuilds earlier than Release 12.1(26)E1 are deferred.

Feature Set	Image Filename	Orderable Product Number[1]
Enterprise: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2, DECnet Phase IV, and VINES routing • DECnet Phase V and CLNS/OSI routing	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-js-mz.121-26.E9	S6S22ALV-12126E
	Supports FlexWAN and OSM: c6sup22-jsv-mz.121-26.E9	S6S22AV-12126E
	Supports SSHv2: c6sup22-jk2s-mz.121-26.E9	S6S22ALK2-12126E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-jk2sv-mz.121-26.E9	S6S22AK2-12126E
	Supports FlexWAN, OSM, and firewall: c6sup22-jo3sv-mz.121-26.E9	S6S22AVH-12126E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-jk2o3sv-mz.121-26.E9	S6S22ZVH-12126E
	Supervisor Engine 1/MSFC2 images	
	c6sup12-js-mz.121-26.E9	S6S12A-12126E
	Supports FlexWAN and OSM: c6sup12-jsv-mz.121-26.E9	S6S12AV-12126E
	Supports SSHv2: c6sup12-jk2s-mz.121-26.E9	S6S12ALK2-12126E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-jk2sv-mz.121-26.E9	S6S12AK2-12126E
	Supports FlexWAN, OSM, and firewall: c6sup12-jo3sv-mz.121-26.E9	S6S12AVH-12126E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-jk2o3sv-mz.121-26.E9	S6S12AK2H-12126E
	Supervisor Engine 1/MSFC images	
	c6sup11-js-mz.121-26.E9	S6S11A-12126E
	Supports FlexWAN and OSM: c6sup11-jsv-mz.121-26.E9	S6S11AV-12126E
	Supports SSHv2: c6sup11-jk2sv-mz.121-26.E9	S6S11ALK2-12126E
	Supports FlexWAN, OSM, and SSHv2: c6sup11-jk2sv-mz.121-26.E9	S6S11AK2-12126E

Feature Set	Image Filename	Orderable Product Number[1]
Desktop (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2 and DECnet Phase IV routing	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-26.E9	S6S22BV-12126E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-26.E9	S6S12BV-12126E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-26.E9	S6S11BV-12126E
Service Provider: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP)	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-ps-mz.121-26.E9	S6S22ZLV-12126E
	Supports FlexWAN and OSM: c6sup22-psv-mz.121-26.E9	S6S22ZV-12126E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-pk2sv-mz.121-26.E9	S6S22ZK2-12126E
	Supports FlexWAN, OSM, and firewall: c6sup22-po3sv-mz.121-26.E9	S6S22ZVH-12126E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-pk2o3sv-mz.121-26.E9	S6S22ZK2H-12126E
	Supervisor Engine 1/MSFC2 image	
	c6sup12-ps-mz.121-26.E9	S6S12ZLV-12126E
	Supports FlexWAN and OSM: c6sup12-psv-mz.121-26.E9	S6S12ZV-12126E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-pk2sv-mz.121-26.E9	S6S12ZK2-12126E
	Supports FlexWAN, OSM, and firewall: c6sup12-po3sv-mz.121-26.E9	S6S12ZVH-12126E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-pk2o3sv-mz.121-26.E9	S6S12ZK2H-12126E
	Supervisor Engine 1/MSFC image	
	c6sup11-ps-mz.121-26.E9	S6S11ZLV-12126E
	Supports FlexWAN and OSM: c6sup11-psv-mz.121-26.E9	S6S11ZV-12126E
	Supports FlexWAN, OSM, and SSHv2: 6sup11-pk2sv-mz.121-26.E9	S6S11ZK2-12126E

Feature Set	Image Filename	Orderable Product Number[1]
IP/IPX (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-26.E9	S6S22DV-12126E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-26.E9	S6S12DV-12126E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-26.E9	S6S11DV-12126E
MSFC2 boot loader	c6msfc2-boot-mz.121-26.E9	N/A
MSFC1 boot loader	c6msfc-boot-mz.121-26.E9	N/A

1. Installed; append with "=" for spare on shipable media.

Release 12.1(23)E4

Note

- For information about the size of Release 12.1(23)E4 images, see the "Image Names and Sizes in Release 12.1(23)E4" section.
- Release 12.1(23)E and rebuilds earlier than Release 12.1(23)E3 are deferred.

Feature Set	Image Filename	Orderable Product Number[1]
Enterprise: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2, DECnet Phase IV, and VINES routing • DECnet Phase V and CLNS/OSI routing	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-js-mz.121-23.E4	S6S22ALV-12123E
	Supports FlexWAN and OSM: c6sup22-jsv-mz.121-23.E4	S6S22AV-12123E
	Supports SSHv2: c6sup22-jk2s-mz.121-23.E4	S6S22ALK2-12123E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-jk2sv-mz.121-23.E4	S6S22AK2-12123E
	Supports FlexWAN, OSM, and firewall: c6sup22-jo3sv-mz.121-23.E4	S6S22AVH-12123E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-jk2o3sv-mz.121-23.E4	S6S22ZVH-12123E
	Supervisor Engine 1/MSFC2 images	
	c6sup12-js-mz.121-23.E4	S6S12A-12123E
	Supports FlexWAN and OSM: c6sup12-jsv-mz.121-23.E4	S6S12AV-12123E
	Supports SSHv2: c6sup12-jk2s-mz.121-23.E4	S6S12ALK2-12123E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-jk2sv-mz.121-23.E4	S6S12AK2-12123E
	Supports FlexWAN, OSM, and firewall: c6sup12-jo3sv-mz.121-23.E4	S6S12AVH-12123E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-jk2o3sv-mz.121-23.E4	S6S12AK2H-12123E
	Supervisor Engine 1/MSFC images	
	c6sup11-js-mz.121-23.E4	S6S11A-12123E
	Supports FlexWAN and OSM: c6sup11-jsv-mz.121-23.E4	S6S11AV-12123E
	Supports SSHv2: c6sup11-jk2sv-mz.121-23.E4	S6S11ALK2-12123E
	Supports FlexWAN, OSM, and SSHv2: c6sup11-jk2sv-mz.121-23.E4	S6S11AK2-12123E

Feature Set	Image Filename	Orderable Product Number[1]
Desktop (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2 and DECnet Phase IV routing	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-23.E4	S6S22BV-12123E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-23.E4	S6S12BV-12123E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-23.E4	S6S11BV-12123E
Service Provider: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP)	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-ps-mz.121-23.E4	S6S22ZLV-12123E
	Supports FlexWAN and OSM: c6sup22-psv-mz.121-23.E4	S6S22ZV-12123E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-pk2sv-mz.121-23.E4	S6S22ZK2-12123E
	Supports FlexWAN, OSM, and firewall: c6sup22-po3sv-mz.121-23.E4	S6S22ZVH-12123E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-pk2o3sv-mz.121-23.E4	S6S22ZK2H-12123E
	Supervisor Engine 1/MSFC2 image	
	c6sup12-ps-mz.121-23.E4	S6S12ZLV-12123E
	Supports FlexWAN and OSM: c6sup12-psv-mz.121-23.E4	S6S12ZV-12123E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-pk2sv-mz.121-23.E4	S6S12ZK2-12123E
	Supports FlexWAN, OSM, and firewall: c6sup12-po3sv-mz.121-23.E4	S6S12ZVH-12123E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-pk2o3sv-mz.121-23.E4	S6S12ZK2H-12123E
	Supervisor Engine 1/MSFC image	
	c6sup11-ps-mz.121-23.E4	S6S11ZLV-12123E
	Supports FlexWAN and OSM: c6sup11-psv-mz.121-23.E4	S6S11ZV-12123E
	Supports FlexWAN, OSM, and SSHv2: 6sup11-pk2sv-mz.121-23.E4	S6S11ZK2-12123E

Feature Set	Image Filename	Orderable Product Number[1]
IP/IPX (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-23.E4	S6S22DV-12123E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-23.E4	S6S12DV-12123E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-23.E4	S6S11DV-12123E
MSFC2 boot loader	c6msfc2-boot-mz.121-23.E4	N/A
MSFC1 boot loader	c6msfc-boot-mz.121-23.E4	N/A

1. Installed; append with "=" for spare on floppy media.

Release 12.1(22)E6

Note

- For information about the size of Release 12.1(22)E6 images, see the "Image Names and Sizes in Release 12.1(22)E6" section.

- Release 12.1(22)E and rebuilds earlier than Release 12.1(22)E6 are deferred.

Feature Set	Image Filename	Orderable Product Number[1]
Enterprise: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2, DECnet Phase IV, and VINES routing • DECnet Phase V and CLNS/OSI routing	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-js-mz.121-22.E6	S6S22ALV-12122E
	Supports FlexWAN and OSM: c6sup22-jsv-mz.121-22.E6	S6S22AV-12122E
	Supports SSHv2: c6sup22-jk2s-mz.121-22.E6	S6S22ALK2-12122E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-jk2sv-mz.121-22.E6	S6S22AK2-12122E
	Supports FlexWAN, OSM, and firewall: c6sup22-jo3sv-mz.121-22.E6	S6S22AVH-12122E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-jk2o3sv-mz.121-22.E6	S6S22ZVH-12122E
	Supervisor Engine 1/MSFC2 images	
	c6sup12-js-mz.121-22.E6	S6S12A-12122E
	Supports FlexWAN and OSM: c6sup12-jsv-mz.121-22.E6	S6S12AV-12122E
	Supports SSHv2: c6sup12-jk2s-mz.121-22.E6	S6S12ALK2-12122E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-jk2sv-mz.121-22.E6	S6S12AK2-12122E
	Supports FlexWAN, OSM, and firewall: c6sup12-jo3sv-mz.121-22.E6	S6S12AVH-12122E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-jk2o3sv-mz.121-22.E6	S6S12AK2H-12122E
	Supervisor Engine 1/MSFC images	
	c6sup11-js-mz.121-22.E6	S6S11A-12122E
	Supports FlexWAN and OSM: c6sup11-jsv-mz.121-22.E6	S6S11AV-12122E
	Supports SSHv2: c6sup11-jk2sv-mz.121-22.E6	S6S11ALK2-12122E
	Supports FlexWAN, OSM, and SSHv2: c6sup11-jk2sv-mz.121-22.E6	S6S11AK2-12122E

Feature Set	Image Filename	Orderable Product Number[1]
Desktop (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2 and DECnet Phase IV routing	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-22.E6	S6S22BV-12122E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-22.E6	S6S12BV-12122E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-22.E6	S6S11BV-12122E
Service Provider: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP)	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-ps-mz.121-22.E6	S6S22ZLV-12122E
	Supports FlexWAN and OSM: c6sup22-psv-mz.121-22.E6	S6S22ZV-12122E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-pk2sv-mz.121-22.E6	S6S22ZK2-12122E
	Supports FlexWAN, OSM, and firewall: c6sup22-po3sv-mz.121-22.E6	S6S22ZVH-12122E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-pk2o3sv-mz.121-22.E6	S6S22ZK2H-12122E
	Supervisor Engine 1/MSFC2 image	
	c6sup12-ps-mz.121-22.E6	S6S12ZLV-12122E
	Supports FlexWAN and OSM: c6sup12-psv-mz.121-22.E6	S6S12ZV-12122E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-pk2sv-mz.121-22.E6	S6S12ZK2-12122E
	Supports FlexWAN, OSM, and firewall: c6sup12-po3sv-mz.121-22.E6	S6S12ZVH-12122E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-pk2o3sv-mz.121-22.E6	S6S12ZK2H-12122E
	Supervisor Engine 1/MSFC image	
	c6sup11-ps-mz.121-22.E6	S6S11ZLV-12122E
	Supports FlexWAN and OSM: c6sup11-psv-mz.121-22.E6	S6S11ZV-12122E
	Supports FlexWAN, OSM, and SSHv2: 6sup11-pk2sv-mz.121-22.E6	S6S11ZK2-12122E

Feature Set	Image Filename	Orderable Product Number[1]
IP/IPX (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-22.E6	S6S22DV-12122E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-22.E6	S6S12DV-12122E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-22.E6	S6S11DV-12122E
MSFC2 boot loader	c6msfc2-boot-mz.121-22.E6	N/A
MSFC1 boot loader	c6msfc-boot-mz.121-22.E6	N/A

1. Installed; append with "=" for spare on floppy media.

Release 12.1(20)E6

Note

- For information about the size of Release 12.1(20)E6 images, see the "Image Names and Sizes in Release 12.1(20)E6" section.

- Release 12.1(20)E and rebuilds earlier than Release 12.1(20)E6 are deferred.

Feature Set	Image Filename	Orderable Product Number[1]
Enterprise: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2, DECnet Phase IV, and VINES routing • DECnet Phase V and CLNS/OSI routing	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-js-mz.121-20.E6	S6S22ALV-12120E
	Supports FlexWAN and OSM: c6sup22-jsv-mz.121-20.E6	S6S22AV-12120E
	Supports SSHv2: c6sup22-jk2s-mz.121-20.E6	S6S22ALK2-12120E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-jk2sv-mz.121-20.E6	S6S22AK2-12120E
	Supports FlexWAN, OSM, and firewall: c6sup22-jo3sv-mz.121-20.E6	S6S22AVH-12120E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-jk2o3sv-mz.121-20.E6	S6S22ZVH-12120E
	Supervisor Engine 1/MSFC2 images	
	c6sup12-js-mz.121-20.E6	S6S12A-12120E
	Supports FlexWAN and OSM: c6sup12-jsv-mz.121-20.E6	S6S12AV-12120E
	Supports SSHv2: c6sup12-jk2s-mz.121-20.E6	S6S12ALK2-12120E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-jk2sv-mz.121-20.E6	S6S12AK2-12120E
	Supports FlexWAN, OSM, and firewall: c6sup12-jo3sv-mz.121-20.E6	S6S12AVH-12120E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-jk2o3sv-mz.121-20.E6	S6S12AK2H-12120E
	Supervisor Engine 1/MSFC images	
	c6sup11-js-mz.121-20.E6	S6S11A-12120E
	Supports FlexWAN and OSM: c6sup11-jsv-mz.121-20.E6	S6S11AV-12120E
	Supports SSHv2: c6sup11-jk2sv-mz.121-20.E6	S6S11ALK2-12120E
	Supports FlexWAN, OSM, and SSHv2: c6sup11-jk2sv-mz.121-20.E6	S6S11AK2-12120E

Feature Set	Image Filename	Orderable Product Number[1]
Desktop (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2 and DECnet Phase IV routing	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-20.E6	S6S22BV-12120E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-20.E6	S6S12BV-12120E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-20.E6	S6S11BV-12120E
Service Provider: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP)	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-ps-mz.121-20.E6	S6S22ZLV-12120E
	Supports FlexWAN and OSM: c6sup22-psv-mz.121-20.E6	S6S22ZV-12120E
	Supports FlexWAN, OSM, and SSHv2: c6sup22-pk2sv-mz.121-20.E6	S6S22ZK2-12120E
	Supports FlexWAN, OSM, and firewall: c6sup22-po3sv-mz.121-20.E6	S6S22ZVH-12120E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup22-pk2o3sv-mz.121-20.E6	S6S22ZK2H-12120E
	Supervisor Engine 1/MSFC2 image	
	c6sup12-ps-mz.121-20.E6	S6S12ZLV-12120E
	Supports FlexWAN and OSM: c6sup12-psv-mz.121-20.E6	S6S12ZV-12120E
	Supports FlexWAN, OSM, and SSHv2: c6sup12-pk2sv-mz.121-20.E6	S6S12ZK2-12120E
	Supports FlexWAN, OSM, and firewall: c6sup12-po3sv-mz.121-20.E6	S6S12ZVH-12120E
	Supports FlexWAN, OSM, firewall, and SSHv2: c6sup12-pk2o3sv-mz.121-20.E6	S6S12ZK2H-12120E
	Supervisor Engine 1/MSFC image	
	c6sup11-ps-mz.121-20.E6	S6S11ZLV-12120E
	Supports FlexWAN and OSM: c6sup11-psv-mz.121-20.E6	S6S11ZV-12120E
	Supports FlexWAN, OSM, and SSHv2: 6sup11-pk2sv-mz.121-20.E6	S6S11ZK2-12120E

Feature Set	Image Filename	Orderable Product Number[1]
IP/IPX (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-20.E6	S6S22DV-12120E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-20.E6	S6S12DV-12120E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-20.E6	S6S11DV-12120E
MSFC2 boot loader	c6msfc2-boot-mz.121-20.E6	N/A
MSFC1 boot loader	c6msfc-boot-mz.121-20.E6	N/A

1. Installed; append with "=" for spare on floppy media.

Release 12.1(19)E1 and 12.1(19)E1a

Release 12.1(19)E and rebuilds are deferred.

Release 12.1(14)E

Release 12.1(14)E is deferred.

Release 12.1(13)E17

Note

- For information about image sizes, see the "Image Names and Sizes in Release 12.1(13)E17" section.

- Release 12.1(13)E and rebuilds earlier than Release 12.1(13)E16 are deferred.

Feature Set	Image Filename	Orderable Product Number[1]
Enterprise: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2, DECnet Phase IV, and VINES routing • DECnet Phase V and CLNS/OSI routing	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-js-mz.121-13.E17	S6S22ALV-12113E
	Supports FlexWAN and OSM: c6sup22-jsv-mz.121-13.E17	S6S22AV-12113E
	Supports SSH: c6sup22-jk2s-mz.121-13.E17	S6S22ALK2-12113E
	Supports FlexWAN, OSM, and SSH: c6sup22-jk2sv-mz.121-13.E17	S6S22AK2-12113E
	Supports FlexWAN, OSM, and firewall: c6sup22-jo3sv-mz.121-13.E17	S6S22AVH-12113E
	Supports FlexWAN, OSM, firewall, and SSH: c6sup22-jk2o3sv-mz.121-13.E17	S6S22ZVH-12113E
	Supervisor Engine 1/MSFC2 images	
	c6sup12-js-mz.121-13.E17	S6S12A-12113E
	Supports FlexWAN and OSM: c6sup12-jsv-mz.121-13.E17	S6S12AV-12113E
	Supports SSH: c6sup12-jk2s-mz.121-13.E17	S6S12ALK2-12113E
	Supports FlexWAN, OSM, and SSH: c6sup12-jk2sv-mz.121-13.E17	S6S12AK2-12113E
	Supports FlexWAN, OSM, and firewall: c6sup12-jo3sv-mz.121-13.E17	S6S12AVH-12113E
	Supports FlexWAN, OSM, firewall, and SSH: c6sup12-jk2o3sv-mz.121-13.E17	S6S12AK2H-12113E
	Supervisor Engine 1/MSFC images	
	c6sup11-js-mz.121-13.E17	S6S11A-12113E
	Supports FlexWAN and OSM: c6sup11-jsv-mz.121-13.E17	S6S11AV-12113E
	Supports SSH: c6sup11-jk2sv-mz.121-13.E17	S6S11ALK2-12113E
	Supports FlexWAN, OSM, and SSH: c6sup11-jk2sv-mz.121-13.E17	S6S11AK2-12113E

Feature Set	Image Filename	Orderable Product Number[1]
Desktop (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2 and DECnet Phase IV routing	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-13.E17	S6S22BV-12113E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-13.E17	S6S12BV-12113E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-13.E17	S6S11BV-12113E
Service Provider: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP)	**Supervisor Engine 2/MSFC2 images**	
	c6sup22-ps-mz.121-13.E17	S6S22ZLV-12113E
	Supports FlexWAN and OSM: c6sup22-psv-mz.121-13.E17	S6S22ZV-12113E
	Supports FlexWAN, OSM, and SSH: c6sup22-pk2sv-mz.121-13.E17	S6S22ZK2-12113E
	Supports FlexWAN, OSM, and firewall: c6sup22-po3sv-mz.121-13.E17	S6S22ZVH-12113E
	Supports FlexWAN, OSM, firewall, and SSH: c6sup22-pk2o3sv-mz.121-13.E17	S6S22ZK2H-12113E
	Supervisor Engine 1/MSFC2 image	
	c6sup12-ps-mz.121-13.E17	S6S12ZLV-12113E
	Supports FlexWAN and OSM: c6sup12-psv-mz.121-13.E17	S6S12ZV-12113E
	Supports FlexWAN, OSM, and SSH: c6sup12-pk2sv-mz.121-13.E17	S6S12ZK2-12113E
	Supports FlexWAN, OSM, and firewall: c6sup12-po3sv-mz.121-13.E17	S6S12ZVH-12113E
	Supports FlexWAN, OSM, firewall, and SSH: c6sup12-pk2o3sv-mz.121-13.E17	S6S12ZK2H-12113E
	Supervisor Engine 1/MSFC image	
	c6sup11-ps-mz.121-13.E17	S6S11ZLV-12113E
	Supports FlexWAN and OSM: c6sup11-psv-mz.121-13.E17	S6S11ZV-12113E
	Supports FlexWAN, OSM, and SSH: 6sup11-pk2sv-mz.121-13.E17	S6S11ZK2-12113E

Feature Set	Image Filename	Orderable Product Number[1]
IP/IPX (no SSH or firewall support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX	**Supervisor Engine 2/MSFC2 image**	
	Supports FlexWAN and OSM: c6sup22-dsv-mz.121-13.E17	S6S22DV-12113E
	Supervisor Engine 1/MSFC2 image	
	Supports FlexWAN and OSM: c6sup12-dsv-mz.121-13.E17	S6S12DV-12113E
	Supervisor Engine 1/MSFC image	
	Supports FlexWAN and OSM: c6sup11-dsv-mz.121-13.E17	S6S11DV-12113E
MSFC2 boot loader	c6msfc2-boot-mz.121-13.E17	N/A
MSFC1 boot loader	c6msfc-boot-mz.121-13.E17	N/A

1. Installed; append with "=" for spare on floppy media.

Release 12.1(12c)E5

Release 12.1(12c)E and rebuilds are deferred.

Release 12.1(11b)E14

Release 12.1(11b)E and rebuilds are deferred.

Release 12.1(8b)E20

Note

- For information about image sizes, see the "Image Names and Sizes in Release 12.1(8b)E20" section.

- Release 12.1(8b)E and rebuilds earlier than Release 12.1(8b)E19 are deferred.

Feature Set	Image Filename	Orderable Product Number[1]
	Note All images include FlexWAN support. All Supervisor Engine 2 images include OSM support.	
Enterprise: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2, DECnet Phase IV, and VINES routing • DECnet Phase V and CLNS/OSI routing	**Supervisor Engine 2/MSFC2 images**	
	Supervisor Engine 2/MSFC2: c6sup22-jsv-mz.121-8b.E20	S6SU22AV-12108E
	Supervisor Engine 2/MSFC2/SSH: c6sup22-jk2sv-mz.121-8b.E20	S6SU22AK2-12108E
	Supervisor Engine 1/MSFC2 images	
	Supervisor Engine 1/MSFC2: c6sup12-jsv-mz.121-8b.E20	S6SUP12AV-12108E
	Supervisor Engine 1/MSFC2/SSH: c6sup12-jk2sv-mz.121-8b.E20	S6SUP12AK2-12108E
	Supervisor Engine 1/MSFC images	
	Supervisor Engine 1/MSFC1: c6sup11-jsv-mz.121-8b.E20	S6SUP11AV-12108E
	Supervisor Engine 1/MSFC1/SSH: c6sup11-jk2sv-mz.121-8b.E20	S6SUP11AK2-12108E
Desktop (no SSH support): • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX • AppleTalk Phase 1/2 and DECnet Phase IV routing	**Supervisor Engine 2/MSFC2 image**	
	Supervisor Engine 2/MSFC2: c6sup22-dsv-mz.121-8b.E20	S6SU22BV-12108E
	Supervisor Engine 1/MSFC2 image	
	Supervisor Engine 1/MSFC2: c6sup12-dsv-mz.121-8b.E20	S6SUP12BV-12108E
	Supervisor Engine 1/MSFC image	
	Supervisor Engine 1/MSFC1: c6sup11-dsv-mz.121-8b.E20	S6SUP11BV-12108E

Feature Set	Image Filename	Orderable Product Number[1]
	Note All images include FlexWAN support. All Supervisor Engine 2 images include OSM support.	
Service Provider: • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP)	**Supervisor Engine 2/MSFC2 images**	
	Supervisor Engine 2/MSFC2: c6sup22-psv-mz.121-8b.E20	S6SU22ZV-12108E
	Supervisor Engine 2/MSFC2/SSH: c6sup22-pk2sv-mz.121-8b.E20	S6SU22ZK2-12108E
	Supervisor Engine 1/MSFC2 images	
	Supervisor Engine 1/MSFC2: c6sup12-psv-mz.121-8b.E20	S6SUP12ZV-12108E
	Supervisor Engine 1/MSFC2/SSH: c6sup12-pk2sv-mz.121-8b.E20	S6SUP12ZK2-12108E
	Supervisor Engine 1/MSFC images	
	Supervisor Engine 1/MSFC1: c6sup11-psv-mz.121-8b.E20	S6SUP11ZV-12108E
	Supervisor Engine 1/MSFC1/SSH: c6sup11-pk2sv-mz.121-8b.E20	S6SUP11ZK2-12108E
IP/IPX (no SSH support)**:** • Wire speed Layer 2 switching (bridging) • Wire speed Layer 3 switching (routing) for IP (routing protocols include RIPv1, RIPv2, OSPF, IGRP, EIGRP, EGP, BGP4, and IS-IS; multicast routing protocols include PIM version 1 and 2, MBGP/MSDP, IGMP, and RGMP) • With Supervisor Engine 2, IPX routing in software on the MSFC2 • With Supervisor Engine 1, wire speed Layer 3 switching (routing) for IPX	**Supervisor Engine 2/MSFC2 image**	
	Supervisor Engine 2/MSFC2: c6sup22-dsv-mz.121-8b.E12	S6SU22DV-12108E
	Supervisor Engine 1/MSFC2 image	
	Supervisor Engine 1/MSFC2: c6sup12-dsv-mz.121-8b.E20	S6SUP12DV-12108E
	Supervisor Engine 1/MSFC image	
	Supervisor Engine 1/MSFC1: c6sup11-dsv-mz.121-8b.E20	S6SUP11DV-12108E
MSFC2 boot loader	c6msfc2-boot-mz.121-8b.E20	N/A
MSFC1 boot loader	c6msfc-boot-mz.121-8b.E20	N/A

1. Installed—append with "=" for spare on floppy media.

Release 12.1(7a)E6

Release 12.1(7a)E and rebuilds are deferred.

Release 12.1(6)E8

Release 12.1(6)E and rebuilds are deferred.

Release 12.1(5c)E12

Release 12.1(5a)E and rebuilds are deferred.

Release 12.1(4)E1

Release 12.1(4)E and rebuilds are deferred.

Release 12.1(3a)E7

Release 12.1(3a)E and rebuilds are deferred.

Release 12.1(2)E2

Release 12.1(2)E and rebuilds are deferred.

Release 12.1(1)E6

Release 12.1(1)E and rebuilds are deferred.

Image Names and Sizes

For detailed information about image names and sizes, refer to this publication:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/ol_2310s.htm

New Features

Note Except for RPR+ redundancy, the new features in Release 12.1(13)E and later releases might require more memory than is currently available on a Supervisor Engine 1.

These sections describe the new features:

- New Features in Release 12.1(27b)E4, page 54
- New Features in Release 12.1(27b)E3, page 55
- New Features in Release 12.1(27b)E2, page 55
- New Features in Release 12.1(27b)E1, page 55
- New Features in Release 12.1(27b)E, page 56
- New Features in Release 12.1(26)E9, page 56
- New Features in Release 12.1(26)E8, page 56
- New Features in Release 12.1(26)E7, page 57

- New Features in Release 12.1(26)E6, page 57
- New Features in Release 12.1(26)E5, page 57
- New Features in Release 12.1(26)E4, page 58
- New Features in Release 12.1(26)E3, page 58
- New Features in Release 12.1(26)E2, page 58
- New Features in Release 12.1(26)E1, page 59
- New Features in Release 12.1(26)E, page 59
- New Features in Release 12.1(23)E4, page 59
- New Features in Release 12.1(23)E3, page 60
- New Features in Release 12.1(23)E2, page 60
- New Features in Release 12.1(23)E1, page 60
- New Features in Release 12.1(23)E, page 61
- New Features in Release 12.1(22)E6, page 61
- New Features in Release 12.1(22)E5, page 61
- New Features in Release 12.1(22)E4, page 62
- New Features in Release 12.1(22)E3, page 62
- New Features in Release 12.1(22)E2, page 62
- New Features in Release 12.1(22)E1, page 63
- New Features in Release 12.1(22)E, page 63
- New Features in Release 12.1(20)E6, page 63
- New Features in Release 12.1(20)E3, page 64
- New Features in Release 12.1(20)E2, page 64
- New Features in Release 12.1(20)E, page 64
- New Features in Release 12.1(19)E1a, page 65
- New Features in Release 12.1(19)E1, page 65
- New Features in Release 12.1(19)E, page 67
- New Features in Release 12.1(14)E, page 68
- New Features in Release 12.1(13)E17, page 68
- New Features in Release 12.1(13)E16, page 69
- New Features in Release 12.1(13)E15, page 69
- New Features in Release 12.1(13)E14, page 69
- New Features in Release 12.1(13)E13, page 70
- New Features in Release 12.1(13)E12, page 70
- New Features in Release 12.1(13)E11, page 70
- New Features in Release 12.1(13)E10, page 71
- New Features in Release 12.1(13)E9, page 71
- New Features in Release 12.1(13)E8, page 71
- New Features in Release 12.1(13)E7, page 72

- New Features in Release 12.1(13)E6, page 72
- New Features in Release 12.1(13)E5, page 72
- New Features in Release 12.1(13)E4, page 73
- New Features in Release 12.1(13)E3, page 73
- New Features in Release 12.1(13)E1, page 74
- New Features in Release 12.1(13)E, page 75
- New Features in Release 12.1(12c)E5, page 79
- New Features in Release 12.1(12c)E4, page 79
- New Features in Release 12.1(12c)E2, page 79
- New Features in Release 12.1(12c)E1, page 80
- New Features in Release 12.1(11b)E14, page 81
- New Features in Release 12.1(11b)E12, page 81
- New Features in Release 12.1(11b)E11, page 82
- New Features in Release 12.1(11b)E7, page 82
- New Features in Release 12.1(11b)E4, page 82
- New Features in Release 12.1(11b)E3, page 83
- New Features in Release 12.1(11b)E2, page 83
- New Features in Release 12.1(11b)E1, page 83
- New Features in Release 12.1(11b)E, page 84
- New Features in Release 12.1(8b)E20, page 88
- New Features in Release 12.1(8b)E19, page 88
- New Features in Release 12.1(8b)E18, page 89
- New Features in Release 12.1(8b)E16, page 89
- New Features in Release 12.1(8b)E15, page 89
- New Features in Release 12.1(8b)E14, page 90
- New Features in Release 12.1(8b)E13, page 90
- New Features in Release 12.1(8b)E12, page 90
- New Features in Release 12.1(8b)E11, page 91
- New Features in Release 12.1(8b)E10, page 91
- New Features in Release 12.1(8b)E9, page 91
- New Features in Release 12.1(8b)E8, page 92
- New Features in Release 12.1(8b)E7, page 92
- New Features in Release 12.1(8b)E6, page 92
- New Features in Release 12.1(8a)E5, page 93
- New Features in Release 12.1(8a)E4, page 93
- New Features in Release 12.1(8a)E3, page 94
- New Features in Release 12.1(8a)E2, page 94
- New Features in Release 12.1(8a)E, page 95

- New Features in Release 12.1(7a)E6, page 97
- New Features in Release 12.1(7a)E1, page 97
- New Features in Release 12.1(7)E, page 97
- New Features in Release 12.1(6)E8, page 98
- New Features in Release 12.1(6)E1, page 98
- New Features in Release 12.1(6)E, page 99
- New Features in Release 12.1(5c)E12, page 99
- New Features in Release 12.1(5c)E10, page 100
- New Features in Release 12.1(5c)E9, page 100
- New Features in Release 12.1(5c)E8, page 100
- New Features in Release 12.1(5a)E3, page 101
- New Features in Release 12.1(5a)E1, page 101
- New Features in Release 12.1(4)E1, page 102
- New Features in Release 12.1(3a)E7, page 102
- New Features in Release 12.1(3a)E4, page 103
- New Features in Release 12.1(3a)E3, page 103
- New Features in Release 12.1(2)E2, page 104
- New Features in Release 12.1(2)E, page 104
- New Features in Release 12.1(1)E6, page 106
- New Features in Release 12.1(1)E2, page 106
- New Features in Release 12.1(1)E, page 107
- New Features in Earlier Releases, page 107

New Features in Release 12.1(27b)E4

These sections describe the new features in Release 12.1(27b)E4, 04 Mar 2008:

- New Hardware Features in Release 12.1(27b)E4, page 54
- New Software Features in Release 12.1(27b)E4, page 54

New Hardware Features in Release 12.1(27b)E4

None.

New Software Features in Release 12.1(27b)E4

None.

New Features in Release 12.1(27b)E3

These sections describe the new features in Release 12.1(27b)E3, 10 Aug 2007:

- New Hardware Features in Release 12.1(27b)E3, page 55
- New Software Features in Release 12.1(27b)E3, page 55

New Hardware Features in Release 12.1(27b)E3

None.

New Software Features in Release 12.1(27b)E3

None.

New Features in Release 12.1(27b)E2

These sections describe the new features in Release 12.1(27b)E2, 12 Jun 2007:

- New Hardware Features in Release 12.1(27b)E2, page 55
- New Software Features in Release 12.1(27b)E2, page 55

New Hardware Features in Release 12.1(27b)E2

None.

New Software Features in Release 12.1(27b)E2

None.

New Features in Release 12.1(27b)E1

These sections describe the new features in Release 12.1(27b)E1, 13 Oct 2006:

- New Hardware Features in Release 12.1(27b)E1, page 55
- New Software Features in Release 12.1(27b)E1, page 55

New Hardware Features in Release 12.1(27b)E1

None.

New Software Features in Release 12.1(27b)E1

None.

New Features in Release 12.1(27b)E

These sections describe the new features in Release 12.1(27b)E, 02 Mar 2006:

- New Hardware Features in Release 12.1(27b)E, page 56
- New Software Features in Release 12.1(27b)E, page 56

New Hardware Features in Release 12.1(27b)E

None.

New Software Features in Release 12.1(27b)E

None.

New Features in Release 12.1(26)E9

These sections describe the new features in Release 12.1(26)E9, 10 Aug 2007:

- New Hardware Features in Release 12.1(26)E9, page 56
- New Software Features in Release 12.1(26)E9, page 56

New Hardware Features in Release 12.1(26)E9

None.

New Software Features in Release 12.1(26)E9

None.

New Features in Release 12.1(26)E8

These sections describe the new features in Release 12.1(26)E8, 22 Jan 2007:

- New Hardware Features in Release 12.1(26)E8, page 56
- New Software Features in Release 12.1(26)E8, page 56

New Hardware Features in Release 12.1(26)E8

None.

New Software Features in Release 12.1(26)E8

None.

New Features in Release 12.1(26)E7

These sections describe the new features in Release 12.1(26)E7, 08 Jun 2006:

- New Hardware Features in Release 12.1(26)E7, page 57
- New Software Features in Release 12.1(26)E7, page 57

New Hardware Features in Release 12.1(26)E7

None.

New Software Features in Release 12.1(26)E7

None.

New Features in Release 12.1(26)E6

These sections describe the new features in Release 12.1(26)E6, 06 Feb 2006:

- New Hardware Features in Release 12.1(26)E6, page 57
- New Software Features in Release 12.1(26)E6, page 57

New Hardware Features in Release 12.1(26)E6

None.

New Software Features in Release 12.1(26)E6

None.

New Features in Release 12.1(26)E5

These sections describe the new features in Release 12.1(26)E5, 05 Jan 2006:

- New Hardware Features in Release 12.1(26)E5, page 57
- New Software Features in Release 12.1(26)E5, page 57

New Hardware Features in Release 12.1(26)E5

None.

New Software Features in Release 12.1(26)E5

None.

New Features in Release 12.1(26)E4

These sections describe the new features in Release 12.1(26)E4, 20 Oct 2005:

- New Hardware Features in Release 12.1(26)E4, page 58
- New Software Features in Release 12.1(26)E4, page 58

New Hardware Features in Release 12.1(26)E4

None.

New Software Features in Release 12.1(26)E4

None.

New Features in Release 12.1(26)E3

These sections describe the new features in Release 12.1(26)E3, 22 Aug 2005:

- New Hardware Features in Release 12.1(26)E3, page 58
- New Software Features in Release 12.1(26)E3, page 58

New Hardware Features in Release 12.1(26)E3

None.

New Software Features in Release 12.1(26)E3

None.

New Features in Release 12.1(26)E2

These sections describe the new features in Release 12.1(26)E2, 30 Jun 2005:

- New Hardware Features in Release 12.1(26)E2, page 58
- New Software Features in Release 12.1(26)E2, page 58

New Hardware Features in Release 12.1(26)E2

None.

New Software Features in Release 12.1(26)E2

None.

New Features in Release 12.1(26)E1

These sections describe the new features in Release 12.1(26)E1, 28 Mar 2005:

- New Hardware Features in Release 12.1(26)E1, page 59
- New Software Features in Release 12.1(26)E1, page 59

New Hardware Features in Release 12.1(26)E1

None.

New Software Features in Release 12.1(26)E1

None.

New Features in Release 12.1(26)E

These sections describe the new features in Release 12.1(26)E, 10 Jan 2005:

- New Hardware Features in Release 12.1(26)E, page 59
- New Software Features in Release 12.1(26)E, page 59

New Hardware Features in Release 12.1(26)E

None.

New Software Features in Release 12.1(26)E

None.

New Features in Release 12.1(23)E4

These sections describe the new features in Release 12.1(23)E4, 29 Aug 2005:

- New Hardware Features in Release 12.1(23)E3, page 60
- New Software Features in Release 12.1(23)E3, page 60

New Hardware Features in Release 12.1(23)E4

None.

New Software Features in Release 12.1(23)E4

None.

New Features in Release 12.1(23)E3

These sections describe the new features in Release 12.1(23)E3, 05 May 2005:

- New Hardware Features in Release 12.1(23)E3, page 60
- New Software Features in Release 12.1(23)E3, page 60

New Hardware Features in Release 12.1(23)E3

None.

New Software Features in Release 12.1(23)E3

None.

New Features in Release 12.1(23)E2

These sections describe the new features in Release 12.1(23)E2, 04 Nov 2004:

- New Hardware Features in Release 12.1(23)E2, page 60
- New Software Features in Release 12.1(23)E2, page 60

New Hardware Features in Release 12.1(23)E2

None.

New Software Features in Release 12.1(23)E2

None.

New Features in Release 12.1(23)E1

These sections describe the new features in Release 12.1(23)E1, 16 Sep 2004:

- New Hardware Features in Release 12.1(23)E1, page 60
- New Software Features in Release 12.1(23)E1, page 60

New Hardware Features in Release 12.1(23)E1

None.

New Software Features in Release 12.1(23)E1

None.

New Features in Release 12.1(23)E

These sections describe the new features in Release 12.1(23)E, 29 Jul 2004:

- New Hardware Features in Release 12.1(23)E, page 61
- New Software Features in Release 12.1(23)E, page 61

New Hardware Features in Release 12.1(23)E

None.

New Software Features in Release 12.1(23)E

- Support for the **mls netflow maximum-flows** command. (CSCee28200)
- Support for the **mls netflow usage notify** global configuration mode command to configure NetFlow table usage monitoring. (CSCdz64998)
- Support in the **show mls statistics** command for display of the approximate Layer 2 switching rate in packets-per-second. (CSCee28215, CSCee92338)
- Support for the **mls ip pbr null0** command, which provides PFC-hardware support for policy-based routing (PBR) configured with a **set interface Null0** command in the route-map. (CSCee73959)

New Features in Release 12.1(22)E6

These sections describe the new features in Release 12.1(22)E6, 05 May 2005:

- New Hardware Features in Release 12.1(22)E6, page 61
- New Software Features in Release 12.1(22)E6, page 61

New Hardware Features in Release 12.1(22)E6

None.

New Software Features in Release 12.1(22)E6

None.

New Features in Release 12.1(22)E5

These sections describe the new features in Release 12.1(22)E5, 20 Jan 2005:

- New Hardware Features in Release 12.1(22)E5, page 61
- New Software Features in Release 12.1(22)E5, page 62

New Hardware Features in Release 12.1(22)E5

None.

New Software Features in Release 12.1(22)E5

None.

New Features in Release 12.1(22)E4

These sections describe the new features in Release 12.1(22)E4, 06 Dec 2004:

- New Hardware Features in Release 12.1(22)E4, page 62
- New Software Features in Release 12.1(22)E4, page 62

New Hardware Features in Release 12.1(22)E4

None.

New Software Features in Release 12.1(22)E4

None.

New Features in Release 12.1(22)E3

These sections describe the new features in Release 12.1(22)E3, 14 Oct 2004:

- New Hardware Features in Release 12.1(22)E3, page 62
- New Software Features in Release 12.1(22)E3, page 62

New Hardware Features in Release 12.1(22)E3

None.

New Software Features in Release 12.1(22)E3

- Support for the **mls ip pbr null0** command, which provides PFC-hardware support for policy-based routing (PBR) configured with a **set interface Null0** command in the route-map. (CSCee73959)

New Features in Release 12.1(22)E2

These sections describe the new features in Release 12.1(22)E2, 10 Jun 2004:

- New Hardware Features in Release 12.1(22)E2, page 62
- New Software Features in Release 12.1(22)E2, page 63

New Hardware Features in Release 12.1(22)E2

None.

New Software Features in Release 12.1(22)E2

None.

New Features in Release 12.1(22)E1

These sections describe the new features in Release 12.1(22)E1, 20 Apr 2004:

- New Hardware Features in Release 12.1(22)E1, page 63
- New Software Features in Release 12.1(22)E1, page 63

New Hardware Features in Release 12.1(22)E1

None.

New Software Features in Release 12.1(22)E1

None.

New Features in Release 12.1(22)E

These sections describe the new features in Release 12.1(22)E, 22 Mar 2004:

- New Hardware Features in Release 12.1(22)E, page 63
- New Software Features in Release 12.1(22)E, page 63

New Hardware Features in Release 12.1(22)E

None.

New Software Features in Release 12.1(22)E

- Support for the **mls qos trust** [**dscp** | **ip-precedence** | **cos**] command on WS-X6148-RJ-45, WS-X6148-RJ-45V, WS-X6148-RJ-21, and WS-X6148-RJ-21V switching modules. (CSCec30649)

New Features in Release 12.1(20)E6

These sections describe the new features in Release 12.1(20)E6, 12 May 2005:

- New Hardware Features in Release 12.1(20)E6, page 63
- New Software Features in Release 12.1(20)E6, page 64

New Hardware Features in Release 12.1(20)E6

None.

New Software Features in Release 12.1(20)E6

None.

New Features in Release 12.1(20)E3

These sections describe the new features in Release 12.1(20)E3, 20 Apr 2004:

- New Hardware Features in Release 12.1(20)E3, page 64
- New Software Features in Release 12.1(20)E3, page 64

New Hardware Features in Release 12.1(20)E3

None.

New Software Features in Release 12.1(20)E3

None.

New Features in Release 12.1(20)E2

These sections describe the new features in Release 12.1(20)E2, 02 Feb 2004:

- New Hardware Features in Release 12.1(20)E2, page 64
- New Software Features in Release 12.1(20)E2, page 64

New Hardware Features in Release 12.1(20)E2

- 1000BASE-DWDM GBIC (DWDM-GBIC)

New Software Features in Release 12.1(20)E2

- Support for the **mls qos trust** [**dscp** | **ip-precedence** | **cos**] command on WS-X6148-RJ-45, WS-X6148-RJ-45V, WS-X6148-RJ-21, and WS-X6148-RJ-21V switching modules. (CSCec30649)

New Features in Release 12.1(20)E

These sections describe the new features in Release 12.1(20)E, 27 Oct 2003:

- New Hardware Features in Release 12.1(20)E, page 64
- New Software Features in Release 12.1(20)E, page 65

New Hardware Features in Release 12.1(20)E

- 1,400 W AC power supply (PWR-1400-AC)

New Software Features in Release 12.1(20)E

- Custom IEEE 802.1Q Ethertypes—Refer to this publication:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/layer2.htm#1054196

New Features in Release 12.1(19)E1a

These sections describe the new features in Release 12.1(19)E1a, 06 Aug 2003:

- New Hardware Features in Release 12.1(19)E1a, page 65
- New Software Features in Release 12.1(19)E1a, page 65

Note Release 12.1(19)E1a images are posted on the LAN Switching Software page at this URL:
http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-sup-ios
Release 12.1(19)E1a images are not posted on the Cisco IOS Upgrade Planner page.

New Hardware Features in Release 12.1(19)E1a

None.

New Software Features in Release 12.1(19)E1a

To change the default for the **link-status event** command to **enabled** on all interfaces on the system:

```
router(config)# [no] logging event link-status default
```

To suppress the link-status event messages during system initialization:

```
router(config)# [no] logging event link-status boot
```

Refer to the following publication for more information:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/i1.htm#wp1338912

New Features in Release 12.1(19)E1

These sections describe the new features in Release 12.1(19)E1, 01 Jul 2003:

- New Hardware Features in Release 12.1(19)E1, page 66
- New Software Features in Release 12.1(19)E1, page 67

New Hardware Features in Release 12.1(19)E1

- 16-port Gigabit Ethernet switching module, fabric-enabled (WS-X6516A-GBIC)
- 48-port 10/100/1000 Mbps switching module, fabric-enabled (WS-X6548-GE-TX; WS-X6548V-GE-TX provides inline power to IP telephones with WS-F6K-VPWR-GE).

Note The WS-X6548-GE-TX and WS-X6548V-GE-TX do not support the following:
—More than 1 Gbps of traffic per EtherChannel
—WS-F6K-DFC
—ISL trunking
—Jumbo frames
—802.1Q tunneling
—Traffic storm control

- 48-port 10/100/1000 Mbps switching module (WS-X6148-GE-TX; WS-X6148V-GE-TX provides inline power to IP telephones with WS-F6K-VPWR-GE).

Note The WS-X6148-GE-TX and WS-X6148V-GE-TX do not support the following:
—More than 1 Gbps of traffic per EtherChannel
—WS-F6K-DFC
—ISL trunking
—Jumbo frames
—802.1Q tunneling
—Traffic storm control

Note The 48-port 10/100/1000 Mbps switching modules (WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX) support these Time Domain Reflectometer commands:

- **test cable-diagnostics tdr**—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/s1.htm#78313

- **show cable-diagnostics tdr**—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/show1.htm#86856

- NAM-2 (WS-SVC-NAM-2) and NAM-1 (WS-SVC-NAM-1) with Supervisor Engine 1 and MSFC2— Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_15353.htm

- SSL Services Module (WS-SVC-SSL-1) with Supervisor Engine 1 and MSFC2— Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3396.htm

- Intrusion Detection System Module 2 (WS-SVC-IDS2-BUN-K9) with Supervisor Engine 1 and MSFC2—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/15620_01.htm

- WS-C6509-NEB-A chassis

New Software Features in Release 12.1(19)E1

- The [**no**] **mls ip multicast** command was extended to FlexWAN module ATM subinterfaces. (CSCeb29878)

New Features in Release 12.1(19)E

These sections describe the new features in Release 12.1(19)E, 03 Jun 2003:

- New Hardware Features in Release 12.1(19)E, page 67
- New Software Features in Release 12.1(19)E, page 67

New Hardware Features in Release 12.1(19)E

- 4000 W DC-power supply (PWR-4000-DC)

New Software Features in Release 12.1(19)E

- Secure Shell (SSH) Version 2 server support in k2 images

  By default, the k2 images support both SSHv1 connections and SSHv2 connections. To restrict connections to either SSHv1 or SSHv2, enter the **ip ssh mode** [**v1** | **v2**] global configuration mode command. Except for the **v1** and **v2** keywords for the **ip ssh mode** command, you configure SSHv2 the same as SSHv1. Refer to this publication for more information:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/sshv1.htm

  For information about SSHv1 client support, refer to the following publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sshv1c.htm
- Support for embedded CiscoView—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/intro.htm#1026452
- Enhancements to the **interface range** command:
  - Support for VLAN interface creation
  - Support for VLAN interface deletion
  - Support for loopback, tunnel, and POS interfaces
- PFC QoS support for time-based Cisco IOS ACLs
- PFC QoS support for queueing-only mode—Refer to the **mls qos queueing-only** command at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/qos.htm#1339834
- MPLS VPN support on the OSM-2OC12-ATM module
- MPLS/VPN support on the OC48/1DPT OSM in DPT mode
- MAC address move notification—Refer to the **mac-address-table notification mac-move** command at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/secure.htm#1079180

Note The MAC address move notification feature does not generate a notification when a new MAC address is added to the CAM or when a MAC address is removed from the CAM.

New Features in Release 12.1(14)E

Note All images in Release 12.1(14)E have been deferred.

These sections describe the new features in Release 12.1(14)E, 16 Dec 2002:

- New Hardware Features in Release 12.1(14)E, page 68
- New Software Features in Release 12.1(14)E, page 68

New Hardware Features in Release 12.1(14)E

- Intrusion Detection System Module 2 (WS-SVC-IDS2-BUN-K9) with Supervisor Engine 2—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/15620_01.htm

New Software Features in Release 12.1(14)E

- Unknown unicast flood protection—Refer to the **mac-address-table unicast-flood** command at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/secure.htm
- Embedded CiscoView support—Refer to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/intro.htm#1026452

New Features in Release 12.1(13)E17

These sections describe the new features in Release 12.1(13)E17, 09 Sep 2005:

- New Hardware Features in Release 12.1(13)E17, page 68
- New Software Features in Release 12.1(13)E17, page 68

New Hardware Features in Release 12.1(13)E17

None.

New Software Features in Release 12.1(13)E17

None.

New Features in Release 12.1(13)E16

These sections describe the new features in Release 12.1(13)E16, 10 May 2005:

- New Hardware Features in Release 12.1(13)E16, page 69
- New Software Features in Release 12.1(13)E16, page 69

New Hardware Features in Release 12.1(13)E16

None.

New Software Features in Release 12.1(13)E16

None.

New Features in Release 12.1(13)E15

These sections describe the new features in Release 12.1(13)E15, 12 Aug 2004:

- New Hardware Features in Release 12.1(13)E15, page 69
- New Software Features in Release 12.1(13)E15, page 69

New Hardware Features in Release 12.1(13)E15

None.

New Software Features in Release 12.1(13)E15

None.

New Features in Release 12.1(13)E14

These sections describe the new features in Release 12.1(13)E14, 31 Mar 2004:

- New Hardware Features in Release 12.1(13)E14, page 69
- New Software Features in Release 12.1(13)E14, page 69

New Hardware Features in Release 12.1(13)E14

None.

New Software Features in Release 12.1(13)E14

None.

New Features in Release 12.1(13)E13

These sections describe the new features in Release 12.1(13)E13, 19 Jan 2004:

- New Hardware Features in Release 12.1(13)E13, page 70
- New Software Features in Release 12.1(13)E13, page 70

New Hardware Features in Release 12.1(13)E13

None.

New Software Features in Release 12.1(13)E13

- Support for the **mls qos trust** [**dscp** | **ip-precedence** | **cos**] command on WS-X6148-RJ-45, WS-X6148-RJ-45V, WS-X6148-RJ-21 and WS-X6148-RJ-21V switching modules. (CSCec30649)

New Features in Release 12.1(13)E12

These sections describe the new features in Release 12.1(13)E12, 24 Nov 2003:

- New Hardware Features in Release 12.1(13)E12, page 70
- New Software Features in Release 12.1(13)E12, page 70

New Hardware Features in Release 12.1(13)E12

None.

New Software Features in Release 12.1(13)E12

None.

New Features in Release 12.1(13)E11

These sections describe the new features in Release 12.1(13)E11, 13 Oct 2003:

- New Hardware Features in Release 12.1(13)E11, page 70
- New Software Features in Release 12.1(13)E11, page 70

New Hardware Features in Release 12.1(13)E11

None.

New Software Features in Release 12.1(13)E11

None.

New Features in Release 12.1(13)E10

These sections describe the new features in Release 12.1(13)E10, 08 Sep 2003:

- New Hardware Features in Release 12.1(13)E10, page 71
- New Software Features in Release 12.1(13)E10, page 71

New Hardware Features in Release 12.1(13)E10

None.

New Software Features in Release 12.1(13)E10

None.

New Features in Release 12.1(13)E9

These sections describe the new features in Release 12.1(13)E9, 14 Jul 2003:

- New Hardware Features in Release 12.1(13)E9, page 71
- New Software Features in Release 12.1(13)E9, page 71

New Hardware Features in Release 12.1(13)E9

None.

New Software Features in Release 12.1(13)E9

None.

New Features in Release 12.1(13)E8

These sections describe the new features in Release 12.1(13)E8, 30 Jun 2003:

- New Hardware Features in Release 12.1(13)E8, page 71
- New Software Features in Release 12.1(13)E8, page 71

New Hardware Features in Release 12.1(13)E8

None.

New Software Features in Release 12.1(13)E8

None.

New Features in Release 12.1(13)E7

These sections describe the new features in Release 12.1(13)E7, 23 Jun 2003:

- New Hardware Features in Release 12.1(13)E7, page 72
- New Software Features in Release 12.1(13)E7, page 72

New Hardware Features in Release 12.1(13)E7

None.

New Software Features in Release 12.1(13)E7

None.

New Features in Release 12.1(13)E6

These sections describe the new features in Release 12.1(13)E6, 21 Apr 2003:

- New Hardware Features in Release 12.1(13)E6, page 72
- New Software Features in Release 12.1(13)E6, page 72

New Hardware Features in Release 12.1(13)E6

None.

New Software Features in Release 12.1(13)E6

None.

New Features in Release 12.1(13)E5

These sections describe the new features in Release 12.1(13)E5, 07 Apr 2003:

- New Hardware Features in Release 12.1(13)E5, page 72
- New Software Features in Release 12.1(13)E5, page 72

New Hardware Features in Release 12.1(13)E5

None.

New Software Features in Release 12.1(13)E5

- Support for the [**no**] **mdix auto** command on these switching modules:
  - WS-X6524-100FX-MM
  - WS-X6548-RJ-45

  - WS-X6548-RJ-21

  (CSCdy04156)

- The WAN ports on the OSM-2+4GE-WAN+ module support a minimum allowable shaping rate of 1 MB.

New Features in Release 12.1(13)E4

These sections describe the new features in Release 12.1(13)E4, 03 Feb 2003:

- New Hardware Features in Release 12.1(13)E4, page 73
- New Software Features in Release 12.1(13)E4, page 73

New Hardware Features in Release 12.1(13)E4

- Initial support for the Cisco 7613 Internet Router chassis.

New Software Features in Release 12.1(13)E4

For information on software features supported on the OSMs, refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

- MultiProtocol Label Switching (MPLS) Basic, including Provider (P) and Provider Edge (PE) functionality on OSM-2OC12-ATM-MM, OSM-2OC12-ATM-SI, OSM-2OC12-ATM-MM+, and OSM-2OC12-ATM-SI+ OSMs—Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

- 64-MB linear Flash memory card (MEM-C6K-FLC64M)—Only supported on Supervisor Engine 1. The device name is slot0, and the card works on the currently released ROMMON. For installation information, refer to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/6507_01.htm

New Features in Release 12.1(13)E3

These sections describe the new features in Release 12.1(13)E3, 26 Dec 2002:

- New Hardware Features in Release 12.1(13)E3, page 73
- New Software Features in Release 12.1(13)E3, page 74

New Hardware Features in Release 12.1(13)E3

- Enhanced 4-port Gigabit Ethernet WAN (GBIC) with two Layer 2 LAN ports (OSM-2+4GE-WAN+)
- 12-port channelized DS3 module (OSM-12CT3/T1)
- 1-port OC-12/T1 channelized module (OSM-1CHOC12/T1)
- Cisco 7609-NEB chassis (CISCO7609)

New Software Features in Release 12.1(13)E3

For information on software features supported on the OSMs, refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

- General Packet Radio Service (GPRS) load balancing for the Server Load Balancing (SLB) module—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e13/iosslb13.htm

- Support for 100 switched virtual circuits (SVCs) per OC-12 ATM OSM.
- Hierarchical traffic shaping on GE-WAN ports on the OSM-2+4GE-WAN+.

New Features in Release 12.1(13)E1

These sections describe the new features in Release 12.1(13)E1, 11 Nov 2002:

- New Hardware Features in Release 12.1(13)E1, page 74
- New Software Features in Release 12.1(13)E1, page 74

New Hardware Features in Release 12.1(13)E1

- Enhanced 4-port OC-3 POS OSM (OSM-4OC3-POS-SI+)
- Enhanced 8-port OC-3 POS OSM (OSM-8OC3-POS-SI+, OSM-8OC3-POS-SL+)
- Enhanced 16-port OC-3 POS OSM (OSM-16OC3-POS-SI+)
- Enhanced 1-port OC-48 POS OSM (OSM-1OC48-POS-SS+, OSM-1OC48-POS-SI+, OSM-1OC48-POS-SL+)

New Software Features in Release 12.1(13)E1

For information on software features supported on the OSMs, refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

- Bridging Control Protocol (BCP) on the OC-3, OC-12, and OC-48 POS OSMs—BCP enables forwarding of Ethernet frames over SONET networks and provides a high-speed extension of enterprise LAN backbone traffic through a metropolitan area.
- Bridging of Routed Encapsulations (BRE) on the OC-12 POS OSMs—BRE enables the OC-12 ATM OSM to receive RFC 1483 routed encapsulated packets and forward them as Layer 2 frames. The BRE software license is FR-BRE-7600.
- RFC 1483 hardware bridging support on FlexWAN—Refer to the following URL for configuration information:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/atm.htm#xtocid10

- MPLS/VPN support for ChOC12/DS3 OSM
- MPLS/VPN support for ChOC48/DS3 OSM
- MPLS/VPN support for OC48/1DPT OSM in POS mode
- MPLS/VPN over Frame Relay encapsulation

- Protocol tunneling over EoMPLS—Support for Layer 2 protocol tunneling over an EoMPLS link allows protocol data units (PDUs) (CDP, STP, and VTP) to be tunneled through an MPLS network.
- Route Processor Redundancy+ (RPR+) support for all OSMs
- Hierarchical traffic-shaping support for Frame Relay Encapsulation
- QoS with Frame Relay encapsulation
- DSCP-based WRED
- QoS support for RFC 1483 and BRE

New Features in Release 12.1(13)E

These sections describe the new features in Release 12.1(13)E, 09 Sep 2002:

- New Hardware Features in Release 12.1(13)E, page 75
- New Software Features in Release 12.1(13)E, page 76

New Hardware Features in Release 12.1(13)E

- Communication Media Module (WS-SVC-CMM)—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3137.htm
- Firewall Services module (WS-SVC-FWM-1-K9)—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_14931.htm
- Catalyst 6500 Series Network Analysis Module (WS-SVC-NAM-1 and WS-SVC-NAM-2)—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_14772.htm
- Inline power daughtercard for Cisco IP Phones (WS-F6K-VPWR)
- 1000BASE-T (copper) GBIC (WS-G5483)
- Coarse Wave Division Multiplexer (CWDM) GBICs:
  - CWDM-GBIC-1470(=)
  - CWDM-GBIC-1490(=)
  - CWDM-GBIC-1510(=)
  - CWDM-GBIC-1530(=)
  - CWDM-GBIC-1550(=)
  - CWDM-GBIC-1570(=)
  - CWDM-GBIC-1590(=)
  - CWDM-GBIC-1610(=)
- Initial support in 12.1 E for the 10GBASE-ER serial 1550 nanometers extended-reach Optical Interface Module (OIM) (WS-G6483) for WS-X6502-10GE (previously supported in 12.1EX releases)
- Initial support for the Catalyst 6500 Series SSL Services Module (WS-SVC-SSL-1) with Supervisor Engine 2, refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3396.htm

New Software Features in Release 12.1(13)E

- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.0 and 1.1 (CVDM-C6500)

    CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 and 1.1 (CVDM-SSLSM)

    CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.0 and 1.1 (CVDM-CSM)

    CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

  To access all CiscoView Device Manager documentation, go to this URL:

  http://www.cisco.com/go/cvdm
- Cisco IP Phone Support—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/voip.htm
- Network-Based Application Recognition (NBAR) for LAN ports—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

Note

- NBAR for LAN ports is supported in software on the MSFC2.
- The PFC2 provides hardware support for input ACLs on LAN ports where you configure NBAR.
- When PFC QoS is enabled, the traffic through LAN ports where you configure NBAR passes through the ingress and egress queues and drop thresholds.
- When PFC QoS is enabled, the MSFC2 sets egress CoS equal to egress IP precedence.
- After passing through an ingress queue, all traffic is processed in software on the MSFC2 on LAN ports where you configure NBAR.
- Distributed NBAR is available on FlexWAN interfaces with Release 12.1(6)E and later releases.

- IEEE 802.1X Port-Based Authentication—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/dot1x.htm

  Note The support for IEEE 802.1X port-based authentication includes VLAN assignment.
- Port Security—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/port_sec.htm

- Remote SPAN—For more information, go to this URL:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/span.htm
- MAC address-based traffic blocking—For more information, go to this URL:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/secure.htm
- SNMP ifindex persistence—For more information, go to this URL:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/ifindex.htm
- Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)—For more information, go to this URL:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/spantree.htm
- NDE enhancements:
  - Destination-source-interface and full-interface flow masks
  - NDE version 5 from the PFC2
  - Sampled NetFlow
  - Option for populating additional fields in NDE records:
    - IP address of the next hop router
    - Ingress interface SNMP ifIndex
    - Egress interface SNMP ifIndex
    - Source autonomous system number
    - Destination autonomous system number

  For more information, go to this URL:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/nde.htm
- Other feature enhancements:
  - UDLD syntax changes—For more information, go to this URL:
    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/udld.htm
  - VTP syntax changes—For more information, go to this URL:
    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/vtp.htm
  - Web Cache Communication Protocol (WCCP) input redirection—For more information, go to this URL:
    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/wccp.htm
- New commands:
  - **standby delay minimum reload**
  - **link debounce**
  - **vlan internal allocation policy** {**ascending** | **descending**}
  - **system jumbomtu**
  - **clear catalyst6000 traffic-meter**
- Enhanced commands:
  - **show vlan internal usage** (enhanced to include VLANs used by WAN interfaces)
  - **show vlan id** (enhanced to support entry of a range of VLANs)
  - **show l2protocol-tunnel** (enhanced to support entry of a VLAN ID)

Release 12.1(13)E supports these software features, which were previously supported in 12.1(11b)EX releases:

- Configuration of Layer 2 EtherChannels that include interfaces on different DFC-equipped switching modules (see CSCdt27074 in the "Resolved General Caveats in Release 12.1(13)E" section on page 249.)
- Route Processor Redundancy Plus (RPR+) redundancy—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/redund.htm

  Note In Release 12.1(13)E and later releases, the RPR and RPR+ redundancy features replace EHSA redundancy.

- 4,096 Layer 2 VLANs—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/vlans.htm

  Note Release 12.1(13)E and later releases allow configuration of 4,096 Layer 3 VLAN interfaces. We recommend that you configure a combined total of no more than 2,000 Layer 3 VLAN interfaces and Layer 3 ports on an MSFC2 with either a Supervisor Engine 2 or a Supervisor Engine 1. We recommend that you configure a combined total of no more than 1,000 Layer 3 VLAN interfaces and Layer 3 ports on an MSFC.

- IEEE 802.1Q tunneling—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/dot1qtnl.htm
- IEEE 802.1Q protocol tunneling—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/dot1qtnl.htm
- IEEE 802.1s, multiple spanning tree (MST)—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/spantree.htm
- IEEE 802.1w, rapid reconfiguration of spanning tree—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/spantree.htm
- IEEE 802.3ad, link aggregation control protocol (LACP)—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/channel.htm
- PortFast BPDU filtering—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/stp_enha.htm
- Automatic creation of Layer 3 VLAN interfaces to support VACLs—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/secure.htm
- VACL capture ports can be any Layer 2 Ethernet port in any VLAN—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/secure.htm
- Configurable MTU size on individual physical Layer 3 ports—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/sw_int.htm

- SPAN destination ports can be configured as trunks so that all SPAN traffic is tagged—For more information, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/span.htm

New Features in Release 12.1(12c)E5

These sections describe the new features in Release 12.1(12c)E5, 28 Oct 2002:

- New Hardware Features in Release 12.1(12c)E5, page 79
- New Software Features in Release 12.1(12c)E5, page 79

New Hardware Features in Release 12.1(12c)E5

None.

New Software Features in Release 12.1(12c)E5

None.

New Features in Release 12.1(12c)E4

These sections describe the new features in Release 12.1(12c)E4, 21 Oct 2002:

- New Hardware Features in Release 12.1(12c)E4, page 79
- New Software Features in Release 12.1(12c)E4, page 79

New Hardware Features in Release 12.1(12c)E4

None.

New Software Features in Release 12.1(12c)E4

None.

New Features in Release 12.1(12c)E2

These sections describe the new features in Release 12.1(12c)E2, 26 Aug 2002:

- New Hardware Features in Release 12.1(12c)E2, page 79
- New Software Features in Release 12.1(12c)E2, page 80

New Hardware Features in Release 12.1(12c)E2

None.

New Software Features in Release 12.1(12c)E2

None.

New Features in Release 12.1(12c)E1

These sections describe the new features in Release 12.1(12c)E1, 05 Aug 2002:

- New Hardware Features in Release 12.1(12c)E1, page 80
- New Software Features in Release 12.1(12c)E1, page 80

New Hardware Features in Release 12.1(12c)E1

- Support for the following OSMs:
  - OSM-2OC48/1DPT-SS, -SI, SL—2-port OC-48 DPT/POS with 4 Gigabit Ethernet LAN ports. The OSM-2OC48/1DPT provides either single-port OC-48 DPT or pass-through mode with dual-port OC-48 POS ports.
  - OSM-1CHOC48/T3-SS, -SI—1-port channelized OC-48 with four Gigabit Ethernet LAN ports.
  - OSM-1CHOC12/T3-SI—1-port channelized OC-12 with 4 Gigabit Ethernet LAN ports.
  - OSM-2OC12-ATM-MM+, SI+—2-port enhanced OC-12 ATM with 4 Gigabit Ethernet LAN ports.

  For information about OSMs, refer to the *OSM Installation and Configuration Note* at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm
- 8-Port Multichannel T1/E1 8PRI port adapter (PA-MC-8TE1+)—For information about the PA-MC-8TE1+ port adapter, refer to the *Multichannel STM-1 Port Adapter* publication at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/multicha/8port_t1/index.htm
- 8-port inverse multiplexing over ATM T1/E1 port adapter (PA-A3-8T1IMA, PA-A3-8E1IMA)—For information about the PA-A3-8T1IMA and PA-A3-8E1IMA port adapters, refer to the *Inverse Multiplexing over ATM Port Adapter Installation and Configuration* publication at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/portadpt/atm_port/a3_8t_8e/index.htm

New Software Features in Release 12.1(12c)E1

For information on software features supported on the OSMs, refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

- Order-dependent ACL Merge (ODM) Algorithm for ACLs used for QoS filtering—Refer to the command reference publication for information about the **mls aclmerge algorithm** and **show fm summary** commands and to caveat CSCdw16595. (For security ACLs, see the "New Software Features in Release 12.1(11b)E" section on page 85.)
- RFC 1483 Bridging on the OC-12 ATM OSMs—Supports forwarding of Layer 2 PDUs between the ATM interfaces on the OC-12 ATM OSMs and Ethernet ports.
- Low Latency Queueing (LLQ) on the OC-48 POS and OC-12 ATM OSMs.
- Class-based weighted fair queueing on the enhanced OSMs.
- PFC2 QoS on the OSM-2OC12-ATM-SI/MM+.

- Traffic storm control—Prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.
- Support for the following PFC QoS policy map class commands:
  - **set ip dscp**
  - **set ip precedence**
- Support for the **no mls qos channel-consistency** command, which supports EtherChannels that have interfaces with and without strict-priority queues when QoS is enabled.
- Support for the **mls ip reflect-threshold**, **mls ip delete-threshold**, and **mls ip install-threshold** commands.

New Features in Release 12.1(11b)E14

These sections describe the new features in Release 12.1(11b)E14, 19 Jan 2004:

- New Hardware Features in Release 12.1(11b)E12, page 81
- New Software Features in Release 12.1(11b)E12, page 81

New Hardware Features in Release 12.1(11b)E14

None.

New Software Features in Release 12.1(11b)E14

None.

New Features in Release 12.1(11b)E12

These sections describe the new features in Release 12.1(11b)E12, 23 Jul 2003:

- New Hardware Features in Release 12.1(11b)E12, page 81
- New Software Features in Release 12.1(11b)E12, page 81

New Hardware Features in Release 12.1(11b)E12

None.

New Software Features in Release 12.1(11b)E12

None.

New Features in Release 12.1(11b)E11

These sections describe the new features in Release 12.1(11b)E11, 2 Jan 2003:

- New Hardware Features in Release 12.1(11b)E11, page 82
- New Software Features in Release 12.1(11b)E11, page 82

New Hardware Features in Release 12.1(11b)E11

None.

New Software Features in Release 12.1(11b)E11

None.

New Features in Release 12.1(11b)E7

These sections describe the new features in Release 12.1(11b)E7, 26 Aug 2002:

- New Hardware Features in Release 12.1(11b)E7, page 82
- New Software Features in Release 12.1(11b)E7, page 82

New Hardware Features in Release 12.1(11b)E7

None.

New Software Features in Release 12.1(11b)E7

None.

New Features in Release 12.1(11b)E4

These sections describe the new features in Release 12.1(11b)E4, 3 June 2002:

- New Hardware Features in Release 12.1(11b)E4, page 82
- New Software Features in Release 12.1(11b)E4, page 82

New Hardware Features in Release 12.1(11b)E4

None.

New Software Features in Release 12.1(11b)E4

None.

New Features in Release 12.1(11b)E3

These sections describe the new features in Release 12.1(11b)E3, 13 May 2002:

- New Hardware Features in Release 12.1(11b)E3, page 83
- New Software Features in Release 12.1(11b)E3, page 83

New Hardware Features in Release 12.1(11b)E3

None.

New Software Features in Release 12.1(11b)E3

None.

New Features in Release 12.1(11b)E2

Note All images in Release 12.1(11b)E2 are deferred.

These sections describe the new features in Release 12.1(11b)E2, 15 April 2002:

- New Hardware Features in Release 12.1(11b)E2, page 83
- New Software Features in Release 12.1(11b)E2, page 83

New Hardware Features in Release 12.1(11b)E2

None.

New Software Features in Release 12.1(11b)E2

New **disable-snooping** keyword for the **mac-address-table static** command that can be entered to prevent multicast traffic addressed to a statically configured multicast MAC address from also being sent to all multicast router ports in the same VLAN, regardless of the enable state of IGMP snooping, which allows normal use of IGMP snooping to constrain multicast traffic to other ports.

With IGMP snooping enabled or disabled, all multicast traffic to a static MAC address configured with the **disable-snooping** keyword is sent only to the static MAC address port and not to any multicast router ports in the VLAN. Without the **disable-snooping** keyword, all multicast traffic to a static MAC address is also sent to all multicast router ports in the VLAN. (CSCdw84943)

New Features in Release 12.1(11b)E1

These sections describe the new features in Release 12.1(11b)E1, 25 Mar 2002:

- New Hardware Features in Release 12.1(11b)E1, page 84
- New Software Features in Release 12.1(11b)E1, page 84

New Hardware Features in Release 12.1(11b)E1

None.

New Software Features in Release 12.1(11b)E1

None.

New Features in Release 12.1(11b)E

Note All images in Release 12.1(11b)E have been deferred.

These sections describe the new features in Release 12.1(11b)E, 28 Feb 2002:

- New Hardware Features in Release 12.1(11b)E, page 84
- New Software Features in Release 12.1(11b)E, page 85

New Hardware Features in Release 12.1(11b)E

- Release 12.1(11b)E provides initial support for the Content Services Gateway (CSG) module (WS-SVC-CSG-1).
- Release 12.1(11b)E provides initial support in 12.1E for the following new hardware products (these products were previously supported in 12.1(8a)EX releases):
  - 1-port serial 10-Gigabit Ethernet fabric-enabled switching module (WS-X6502-10GE)
  - 10GBASE-LR serial 1310-nanometer long-haul OIM (WS-G6488) for WS-X6502-10GE
  - 4-port OC-3c/STM-1c POS, SM-IR module (OSM-4OC3-POS-SI)
  - 2-port OC-12 ATM Optical Services Module (OSM-2OC12-ATM-MM, SI)
  - 4-port Gigabit Ethernet WAN module (OSM-4GE-WAN-GBIC)
  - 16-port 10/100/1000BASE-T fabric-enabled Gigabit Ethernet switching module (WS-X6516-GE-TX)
  - 24-port 100FX Ethernet multimode fabric-enabled Fast Ethernet switching module (WS-X6524-100FX-MM)
  - 48-port 10/100TX RJ-21 fabric-enabled Ethernet/Fast Ethernet switching module (WS-X6548-RJ-21)
  - 48-port 10/100TX RJ-21 Ethernet/Fast Ethernet switching module (WS-X6348-RJ-21V)
  - Intrusion Detection System Module (WS-X6381-IDS) with both Supervisor Engine 2 and Supervisor Engine 1 (previous support in 12.1EX releases was only with Supervisor Engine 2).
  - Network Analysis Module (WS-X6380-NAM) with both Supervisor Engine 2 and Supervisor Engine 1 (previous support in 12.1EX releases was only with Supervisor Engine 2).
  - Cisco 7606 chassis, 6 slots (CISCO7606)

    Note The CISCO7606 chassis is supported only with Supervisor Engine 2.

New Software Features in Release 12.1(11b)E

For information on software features supported on the OSMs, refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

Release 12.1(11b)E supports these new features:

- Jumbo frames on all Ethernet ports

Caution The following switching modules support a maximum ingress frame size of 8092 bytes:

- WS-X6516-GE-TX when operating at 100 Mbps
- WS-X6148-RJ-45, WS-X6148-RJ-45V and WS-X6148-RJ21, WS-X6148-RJ21V
- WS-X6248-RJ-45 and WS-X6248-TEL
- WS-X6248A-RJ-45 and WS-X6248A-TEL
- WS-X6348-RJ-45, WS-X6348-RJ45V and WS-X6348-RJ21V

When jumbo frame support is configured, these modules drop ingress frames larger than 8092 bytes.

- Hardware support for directed broadcast in Supervisor Engine 2—For information, refer to the command reference at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/m1.htm#35329

- You can enter the **do** command followed by an EXEC mode command in configuration mode. Be aware of caveat CSCdx02925 (see the "Resolved General Caveats in Release 12.1(12c)E1" section on page 264) and CSCdw92111 (see the "Resolved General Caveats in Release 12.1(13)E" section on page 249).
- With a PFC2, hardware support for directed broadcasts with the **mls ip directed-broadcast** command.
- New commands to show interface capabilities:
  - **show interfaces capabilities** [{**module** *mod_num*}]
  - **show interfaces** {*type interface-number*} **capabilities**
- **fsck** [**/automatic** | **disk0:**] command to check a Flash file system for damage and repair any problems.
- New commands for Protocol Independent Multicast (PIM) scalability and convergence enhancements:
  - [**no**] **ip multicast rpf interval** *interval*

    Use this command to set the reverse path forwarding (RPF) consistency-check interval.
  - [**no**] **ip multicast rpf backoff** {{*min max*} | **disable**}

    Use this command to set the PIM back-off interval.
  - **show ip rpf events**

    Use this command to show the triggered RPP statistics.
- New command to support full CEF load balancing, including Layer 4 ports and Layer 3 source IP and destination IP addresses:

  [**no**] **mls ip cef load-sharing full**

- With Supervisor Engine 2, new command to set the boot-up diagnostic level:

  diagnostic level [**minimal** | **complete** | **bypass**]
- New command to configure the fabric switching mode:

  [**no**] **fabric switching-mode allow** {**bus-mode** | {**truncated** [{**threshold** [*number*]}]}
- New command to make the SFM required for system operation:

  [**no**] **fabric required**
- PortFast support for trunks.
- With a PFC2 (and DFCs, if present), hardware support for policy-based routing (PBR) route-map sequences that use the **set ip default next-hop** keywords.
- PFC2-based QoS for WAN ports on the following OSMs:
  - 4-, 8-, and 16-port OC-3 POS OSMs
  - 2- and 4-port OC-12 POS OSMs
  - 4-port Gigabit Ethernet WAN (GBIC) OSM
- Class-based Weighted Fair Queueing (CBWFQ) on the WAN ports of the following OSMs:
  - 4-, 8-, and 16-port OC-3 POS OSMs
  - 2- and 4-port OC-12 POS OSMs
- Distributed Low Latency Queueing (dLLQ) on the WAN ports of the following OSMs:
  - 4-, 8-, and 16-port OC-3 POS OSMs
  - 2- and 4-port OC-12 POS OSMs
- Frame Relay Encapsulation on the WAN ports of the following OSMs:
  - 4-, 8-, and 16-port OC-3 POS OSMs
  - 2- and 4-port OC-12 POS OSMs
  - Single-port OC-48 POS OSM
  - 4-, and 8-port Channelized OC-12 OSMs
  - Single-, and dual-port Channelized OC-48 OSMs.
- MPLS VPN on the WAN ports of the following OSMs:
  - 4-, 8-, and 16-port OC-3 POS OSMs
  - 2- and 4-port OC-12 POS OSMs
  - Single-port OC-48 POS OSM
  - FlexWAN module (WS-X6182-2PA)

    Note All MPLS features on the FlexWAN module require a Supervisor Engine 2 and MSFC2.

  - 4-port Gigabit Ethernet WAN (GBIC) OSM
- EoMPLS on the Flexwan module (WS-X6182-2PA)

  Note Support for EoMPLS on the FlexWAN module requires a Supervisor Engine 2 and MSFC2.

- IPsec, SSH, and 3DES support for new firewall images.

- Support for the Network Analysis Module with Supervisor Engine 1 and MSFC2.CSCed81316
- Support for RADIUS load balancing and Virtual Private Networking (VPN) load balancing.

Release 12.1(11b)E provides initial support in 12.1E for the following software features (these features were previously supported in 12.1(8a)EX releases):

Note The quoted titles in some of the following items refer to chapters in the software configuration guides:

- *Catalyst 6500 Series Cisco IOS Software Configuration Guide*
- *Cisco 7600 Series Router IOS Software Configuration Guide*

- SPAN with ports on fabric-enabled switching modules. (CSCds02430)
- MultiProtocol Label Switching (MPLS) Basic, including Provider (P) and Provider Edge (PE) functionality—Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

  Note The Ethernet LAN ports do not support MPLS. Only WAN ports support MPLS.

- Ethernet over MPLS—Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm
- VLAN 1 Minimization—"Configuring Layer 2 Ethernet Interfaces"
- VLAN Configuration Mode—"Configuring VLANs"
- Private VLANs—"Configuring Private VLANs"

  Note With PFC2, Release 12.1(11b)E provides Layer 3 switching for multicast traffic in private VLANs and supports IGMP Snooping in private VLANs.

- QoS Data Export—"Configuring QoS"
- Cisco IOS Firewall Feature Set—"Configuring Network Security"
- VLAN Access Control Lists (VACLs)—"Configuring Network Security"
- VACL Deny Logging—"Configuring Network Security"
- Order-Dependent ACL Merge (ODM) Algorithm for security ACLs—Refer to the command reference publication for information about the **mls aclmerge algorithm** and **show fm summary** commands. (For QoS, see the "New Software Features in Release 12.1(12c)E1" section on page 80.)
- Configurable last member query interval for IGMP snooping—Refer to the command reference publication for information about the **ip igmp snooping last-member-query-interval** command.
- Content Switching Module, Software Release 2.2—Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_12569.htm
- Cisco QoS Device Manager (QDM)—Refer to these publications:

  Release and Installation Notes:

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qdm/qdmrn21.htm

  Downloading:

http://www.cisco.com/cgi-bin/tablebuild.pl/qdm

- Troubleshooting DCEF synchronization—The following commands help to troubleshoot DCEF synchronization problems on a Supervisor Engine 2:
  - **ip cef table consistency-check**
  - **show ip cef inconsistency**
  - **clear ip cef epoch full**
  - **clear ip cef inconsistency**
  - Refer to the online publications at these URLs:
  - http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_r/index.htm

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt1/xcfcefc.htm#33123
- Supervisor Engine 2 ROMMON software release 7.1(1), which introduces support for the MEM-C6K-ATA-1-64M= (64MB) PCMCIA ATA FlashDisk device. Refer to the following online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_13488.htm
- If the MSFC address falls within the range of a PBR ACL, traffic addressed to the MSFC is policy routed in hardware instead of being forwarded to the MSFC. To prevent policy routing of traffic addressed to the MSFC, configure PBR ACLs to deny traffic addressed to the MSFC. (CSCse86399)

New Features in Release 12.1(8b)E20

These sections describe the new features in Release 12.1(8b)E20, 09 Sep 2005:

- New Hardware Features in Release 12.1(8b)E20, page 88
- New Software Features in Release 12.1(8b)E20, page 88

New Hardware Features in Release 12.1(8b)E20

None.

New Software Features in Release 12.1(8b)E20

None.

New Features in Release 12.1(8b)E19

These sections describe the new features in Release 12.1(8b)E19, 09 May 2005:

- New Hardware Features in Release 12.1(8b)E19, page 88
- New Software Features in Release 12.1(8b)E19, page 89

New Hardware Features in Release 12.1(8b)E19

None.

New Software Features in Release 12.1(8b)E19

None.

New Features in Release 12.1(8b)E18

These sections describe the new features in Release 12.1(8b)E18, 19 Jan 2004:

- New Hardware Features in Release 12.1(8b)E18, page 89
- New Software Features in Release 12.1(8b)E18, page 89

New Hardware Features in Release 12.1(8b)E18

None.

New Software Features in Release 12.1(8b)E18

None.

New Features in Release 12.1(8b)E16

These sections describe the new features in Release 12.1(8b)E16, 18 Dec 2003:

- New Hardware Features in Release 12.1(8b)E16, page 89
- New Software Features in Release 12.1(8b)E16, page 89

New Hardware Features in Release 12.1(8b)E16

None.

New Software Features in Release 12.1(8b)E16

None.

New Features in Release 12.1(8b)E15

These sections describe the new features in Release 12.1(8b)E15, 22 Jul 2003:

- New Hardware Features in Release 12.1(8b)E15, page 89
- New Software Features in Release 12.1(8b)E15, page 90

New Hardware Features in Release 12.1(8b)E15

None.

New Software Features in Release 12.1(8b)E15

None.

New Features in Release 12.1(8b)E14

These sections describe the new features in Release 12.1(8b)E14, 28 Apr 2003:

- New Hardware Features in Release 12.1(8b)E14, page 90
- New Software Features in Release 12.1(8b)E14, page 90

New Hardware Features in Release 12.1(8b)E14

None.

New Software Features in Release 12.1(8b)E14

- Shortcut-consistency checker—The **mls ip multicast consistency-check** command checks the multicast route table and the multicast hardware entries for consistency and corrects any inconsistencies. (CSCea66040)
- SPAN with ports on fabric-enabled switching modules. (CSCea07663)

New Features in Release 12.1(8b)E13

These sections describe the new features in Release 12.1(8b)E13, 30 Dec 2002:

- New Hardware Features in Release 12.1(8b)E13, page 90
- New Software Features in Release 12.1(8b)E13, page 90

New Hardware Features in Release 12.1(8b)E13

None.

New Software Features in Release 12.1(8b)E13

None.

New Features in Release 12.1(8b)E12

These sections describe the new features in Release 12.1(8b)E12, 28 Oct 2002:

- New Hardware Features in Release 12.1(8b)E12, page 90
- New Software Features in Release 12.1(8b)E12, page 91

New Hardware Features in Release 12.1(8b)E12

None.

New Software Features in Release 12.1(8b)E12

None.

New Features in Release 12.1(8b)E11

These sections describe the new features in Release 12.1(8b)E11, 28 May 2002:

- New Hardware Features in Release 12.1(8b)E11, page 91
- New Software Features in Release 12.1(8b)E11, page 91

New Hardware Features in Release 12.1(8b)E11

None.

New Software Features in Release 12.1(8b)E11

None.

New Features in Release 12.1(8b)E10

These sections describe the new features in Release 12.1(8b)E10, 22 April 2002:

- New Hardware Features in Release 12.1(8b)E10, page 91
- New Software Features in Release 12.1(8b)E10, page 91

New Hardware Features in Release 12.1(8b)E10

None.

New Software Features in Release 12.1(8b)E10

None.

New Features in Release 12.1(8b)E9

These sections describe the new features in Release 12.1(8b)E9, 20 Feb 2002:

- New Hardware Features in Release 12.1(8b)E9, page 91
- New Software Features in Release 12.1(8b)E9, page 92

New Hardware Features in Release 12.1(8b)E9

None.

New Software Features in Release 12.1(8b)E9

None.

New Features in Release 12.1(8b)E8

These sections describe the new features in Release 12.1(8b)E8, 21 Jan 2002:

- New Hardware Features in Release 12.1(8b)E8, page 92
- New Software Features in Release 12.1(8b)E8, page 92

New Hardware Features in Release 12.1(8b)E8

None.

New Software Features in Release 12.1(8b)E8

None.

New Features in Release 12.1(8b)E7

These sections describe the new features in Release 12.1(8b)E7, 17 Dec 2001:

- New Hardware Features in Release 12.1(8b)E7, page 92
- New Software Features in Release 12.1(8b)E7, page 92

New Hardware Features in Release 12.1(8b)E7

Release 12.1(8b)E7 provides initial support for the Cisco 7603 chassis with Supervisor Engine 1 and MSFC2.

New Software Features in Release 12.1(8b)E7

None.

New Features in Release 12.1(8b)E6

These sections describe the new features in Release 12.1(8b)E6, 03 Dec 2001:

- New Hardware Features in Release 12.1(8b)E6, page 92
- New Software Features in Release 12.1(8b)E6, page 93

New Hardware Features in Release 12.1(8b)E6

None.

New Software Features in Release 12.1(8b)E6

Release 12.1(8b)E6 supports these new features:

- The new **show mls cef lookup** command, which displays the longest FIB prefix match (CSCdv64090).
- A FIB to TCAM consistency checker that corrects any inconsistencies discovered, displayed with these commands:
  - **show mls cef logging** (new)
  - **show mls cef hardware** (enhanced)

  (CSCdv76631)

For information about the new and enhanced commands, refer to the online version of the *Catalyst 6500 Series Cisco IOS Command Reference* publication at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/index.htm

New Features in Release 12.1(8a)E5

These sections describe the new features in Release 12.1(8a)E5, 26 Oct 2001:

- New Hardware Features in Release 12.1(8a)E5, page 93
- New Software Features in Release 12.1(8a)E5, page 93

New Hardware Features in Release 12.1(8a)E5

None.

New Software Features in Release 12.1(8a)E5

None.

New Features in Release 12.1(8a)E4

These sections describe the new features in Release 12.1(8a)E4, 17 Sep 2001:

- New Hardware Features in Release 12.1(8a)E4, page 93
- New Software Features in Release 12.1(8a)E4, page 93

New Hardware Features in Release 12.1(8a)E4

None.

New Software Features in Release 12.1(8a)E4

None.

New Features in Release 12.1(8a)E3

These sections describe the new features in Release 12.1(8a)E3, 20 Aug 2001:

- New Hardware Features in Release 12.1(8a)E3, page 94
- New Software Features in Release 12.1(8a)E3, page 94

New Hardware Features in Release 12.1(8a)E3

Release 12.1(8a)E3 provides initial support for these products:

- The following Optical Services Modules:
  - OC-48 POS (OSM-1OC48-POS-SS, -SI, -SL)
  - OC-12 POS (OSM-2OC12-POS-MM, -SI, -SL, OSM-4OC12-POS-MM, -SI, -SL)
  - OC-3 POS (OSM-8OC3-POS-MM, -SI, -SL, OSM-16OC3-POS-MM, -SI, -SL)
  - Channelized OC-48 (OSM-1CHOC48/T3-SS, -SI)
  - Channelized OC-12 (OSM-4CHOC12/T3-SI)

  Refer to this publication about Optical Services Modules:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm
- Cisco 7600 9-slot chassis (supported only with Supervisor Engine 2)
- Cisco 7600 3-slot chassis (supported only with Supervisor Engine 2 in Releases 12.1(8b)E6 and earlier)

New Software Features in Release 12.1(8a)E3

None.

New Features in Release 12.1(8a)E2

These sections describe the new features in Release 12.1(8a)E2, 07 Aug 2001:

- New Hardware Features in Release 12.1(8a)E2, page 94
- New Software Features in Release 12.1(8a)E2, page 94

New Hardware Features in Release 12.1(8a)E2

None.

New Software Features in Release 12.1(8a)E2

None.

New Features in Release 12.1(8a)E

These sections describe the new features in Release 12.1(8a)E, 11 Jul 2001:

- New Hardware Features in Release 12.1(8a)E, page 95
- New Software Features in Release 12.1(8a)E, page 96

Note Release 12.1(8a)E is deferred.

New Hardware Features in Release 12.1(8a)E

Release 12.1(8a)E provides initial Release 12.1 E support for these products:

- Supervisor Engine 2, PFC2, and MSFC2—WS-X6K-S2U-MSFC2 and WS-X6K-S2-MSFC2

  Note Many TFTP implementations cannot transfer 16 MB or larger files. In Release 12.1(8a)E and later releases, system software images for Supervisor Engine 2 are larger than 16 MB. To transfer 16 MB or larger files, you might need to use FTP or rcp. Refer to this online publication for procedures:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt2/fcd203.htm

- Switch Fabric Module—WS-C6500-SFM (does not support 13-slot chassis)
- Switch Fabric Module version 2—WS-X6500-SFM 2 (supports all chassis)
- Switching modules:
  - WS-F6K-DFC—Distributed Forwarding Card
  - WS-X6816-GBIC—16-port Gigabit Ethernet switching module (GBIC, fabric-enabled, dual switch fabric interfaces, DFC-equipped—requires Switch Fabric Module)

    Note The WS-X6816-GBIC switching module is supported only with Supervisor Engine 2 and requires the Switch Fabric Module. In the WS-6513 chassis, it is supported only in slots 9 through 13.

  - WS-X6516-GBIC—16-port Gigabit Ethernet switching module (GBIC, fabric-enabled)
  - WS-X6548-RJ-45—48-port 10/100BASE-T switching module (RJ-45; fabric-enabled)
- Catalyst 13-slot chassis—WS-C6513 (supported only with Supervisor Engine 2)
- Initial support with Supervisor Engine 2 for the Content Switching Module (WS-X6066-SLB-APC). Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_11631.htm
- Initial support with Supervisor Engine 2 for the FlexWAN module (WS-X6182-2PA). Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/flexwan/index.htm

New Software Features in Release 12.1(8a)E

Release 12.1(8a)E supports these new software features:

- Support for source specific multicast with IGMPv3, IGMP v3lite, and URD. For complete information and procedures, refer to this URL:

  http//www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtssm5t.htm

- Support for chassis with reduced MAC address allocation. Refer to the "Configuring STP" chapter in the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/spantree.htm

- The highest value for the **maximum-paths** command has been raised from six to eight.
- Enhanced Unicast RPF for Supervisor Engine 2, PFC2, and MSFC2. Refer to the "Configuring Network Security" chapter in the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/secure.htm

- Backup server farms in Cisco IOS server load balancing. Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e8/iosslb8e.htm

- Enhanced password security. Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e8/8e_md5.htm

- With Supervisor Engine 2, you can configure the MTU size on VLAN interfaces to support jumbo frames. For Supervisor Engine 1, see the "New Software Features in Release 12.1(7)E" section.

Release 12.1(8a)E provides initial support in 12.1E for the following software features (these features were previously supported in 12.1(5c)EX releases):

- IGMP snooping querier
- With Supervisor Engine 2, PFC2, MSFC2, and DFCs, distributed hardware Layer 3 switching:
  - Distributed hardware IP unicast Layer 3 switching
  - Distributed hardware IP multicast Layer 3 switching, including (*,G) flows
- With Supervisor Engine 2, PFC2, MSFC2, support in distributed hardware for these features:
  - Multicast non-RPF traffic processing
  - PBR route-map sequences that use the **match ip address** and **set ip next-hop** keywords (the MSFC2 provides processing in software for route-map sequences that use the **match length** and **set interface** keywords); refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1, "Classification," "Configuring Policy-Based Routing," at this URL:

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt1/qcdpbr.htm

    With Release 12.1(11b)E and later releases, the PFC2 and any DFCs provide hardware support for the **set ip default next-hop** PBR keywords.
  - TCP intercept
  - Enhanced reflexive ACLS
  - IP Unicast RPF

  - WCCP
- With PFC2, dual-rate aggregate policing
- Per-VLAN statistics, displayed with the **show interface vlan** *vlan_ID* **| include Switched** command
- Broadcast suppression for both Layer 3 and Layer 2 interfaces
- With PFC2, Layer 4-based EtherChannel frame distribution

New Features in Release 12.1(7a)E6

These sections describe the new features in Release 12.1(7a)E6, 15 Feb 2002:

- New Hardware Features in Release 12.1(7a)E6, page 97
- New Software Features in Release 12.1(7a)E6, page 97

New Hardware Features in Release 12.1(7a)E6

None.

New Software Features in Release 12.1(7a)E6

None.

New Features in Release 12.1(7a)E1

These sections describe the new features in Release 12.1(7a)E1, 14 May 2001:

- New Hardware Features in Release 12.1(7a)E1, page 97
- New Software Features in Release 12.1(7a)E1, page 97

New Hardware Features in Release 12.1(7a)E1

None.

New Software Features in Release 12.1(7a)E1

None.

New Features in Release 12.1(7)E

These sections describe the new features in Release 12.1(7)E, 30 Apr 2001:

- New Hardware Features in Release 12.1(7)E, page 98
- New Software Features in Release 12.1(7)E, page 98

New Hardware Features in Release 12.1(7)E

Release 12.1(7)E provides initial support with Supervisor Engine 1 for the PA-MC-STM-1 multichannel STM-1 port adapter in the FlexWAN module. Refer to this online publication:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e7/12e_stm.htm

New Software Features in Release 12.1(7)E

Release 12.1(7)E supports these new software features:

- With Supervisor Engine 1, you can configure the MTU size on VLAN interfaces to support jumbo frames. For Supervisor Engine 2, see the "New Software Features in Release 12.1(8a)E" section.
- Release 12.1(7)E provides support for the Route Health Injection feature on the Content Switching Module (WS-X6066-SLB-APC). Refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_11631.htm
- Release 12.1(7)E provides these new Cisco IOS server load balancing (Cisco IOS SLB) features:
  - Multiple Firewall Farm Support
  - Route Health Injection

  Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e7/iosslb7e.htm

New Features in Release 12.1(6)E8

These sections describe the new features in Release 12.1(6)E8, 12 Feb 2002:

- New Hardware Features in Release 12.1(6)E8, page 98
- New Software Features in Release 12.1(6)E8, page 98

New Hardware Features in Release 12.1(6)E8

None.

New Software Features in Release 12.1(6)E8

None.

New Features in Release 12.1(6)E1

These sections describe the new features in Release 12.1(6)E1, 09 Apr 2001:

- New Hardware Features in Release 12.1(6)E1, page 99
- New Software Features in Release 12.1(6)E1, page 99

New Hardware Features in Release 12.1(6)E1

None.

New Software Features in Release 12.1(6)E1

None.

New Features in Release 12.1(6)E

These sections describe the new features in Release 12.1(6)E, 26 Mar 2001:

- New Hardware Features in Release 12.1(6)E, page 99
- New Software Features in Release 12.1(6)E, page 99

New Hardware Features in Release 12.1(6)E

Release 12.1(6)E provides initial support with Supervisor Engine 1 for the Content Switching Module (WS-X6066-SLB-APC). Refer to this publication:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_11631.htm

New Software Features in Release 12.1(6)E

Release 12.1(6)E provides initial support with Supervisor Engine 1 for distributed Network-Based Application Recognition (dNBAR) on FlexWAN module interfaces. dNBAR provides intelligent traffic classification. dNBAR recognizes traffic from a wide variety of applications, including web-based and other difficult-to-classify protocols that use dynamic TCP/UDP port assignments. Refer to this online publication:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e6/dnbar.htm

New Features in Release 12.1(5c)E12

These sections describe the new features in Release 12.1(5c)E12, 13 Feb 2002:

- New Hardware Features in Release 12.1(6)E, page 99
- New Software Features in Release 12.1(6)E, page 99

New Hardware Features in Release 12.1(5c)E12

None.

New Software Features in Release 12.1(5c)E12

None.

New Features in Release 12.1(5c)E10

These sections describe the new features in Release 12.1(5c)E10, 02 Apr 2001:

- New Hardware Features in Release 12.1(5c)E10, page 100
- New Software Features in Release 12.1(5c)E10, page 100

New Hardware Features in Release 12.1(5c)E10

None.

New Software Features in Release 12.1(5c)E10

None.

New Features in Release 12.1(5c)E9

These sections describe the new features in Release 12.1(5c)E9, 27 Mar 2001:

- New Hardware Features in Release 12.1(5c)E10, page 100
- New Software Features in Release 12.1(5c)E10, page 100

New Hardware Features in Release 12.1(5c)E9

None.

New Software Features in Release 12.1(5c)E9

None.

New Features in Release 12.1(5c)E8

These sections describe the new features in Release 12.1(5c)E8, 05 Mar 2001:

- New Hardware Features in Release 12.1(5c)E8, page 100
- New Software Features in Release 12.1(5c)E8, page 100

New Hardware Features in Release 12.1(5c)E8

None.

New Software Features in Release 12.1(5c)E8

None.

New Features in Release 12.1(5a)E3

These sections describe the new features in Release 12.1(5a)E3, 22 Jan 2001:

- New Hardware Features in Release 12.1(5a)E3, page 101
- New Software Features in Release 12.1(5a)E3, page 101

New Hardware Features in Release 12.1(5a)E3

None.

New Software Features in Release 12.1(5a)E3

None.

New Features in Release 12.1(5a)E1

These sections describe the new features in Release 12.1(5a)E1, 28 Dec 2000:

- New Hardware Features in Release 12.1(5a)E1, page 101
- New Software Features in Release 12.1(5a)E1, page 101

New Hardware Features in Release 12.1(5a)E1

Release 12.1(5a)E1 provides initial support with Supervisor Engine 1 for the FlexWAN module (WS-X6182-2PA). Refer to this publication:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/flexwan/index.htm

New Software Features in Release 12.1(5a)E1

- Release 12.1(5a)E1 supports Secure Shell (SSH) Version 1 with 3DES encryption. Refer to these online publications:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/sshv1.htm

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sshv1c.htm
- Distributed MLPPP (dMLPPP) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/index.htm
- Inverse Multiplexing over ATM (IMA) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/index.htm

Note

- Support for mobile IP is restored in Release 12.1(5a)E1.

- To support the requirements of future hardware and provide compatibility with previous releases, the **interface port-channel channel-group** command has been changed to support up to 64 values within the range 1 to 256.
- With Release 12.1(5a)E1 and later:
  - The IP feature set image is replaced with the service provider feature set image, which provides the same features, and includes service provider features.
  - All images include FlexWAN support, which reduces the complexity of image selection and the potential for confusion. You can add a FlexWAN module without an image upgrade. You can use these images whether or not you have a FlexWAN module installed.

New Features in Release 12.1(4)E1

These sections describe the new features in Release 12.1(4)E1, 20 Nov 2000:

- New Hardware Features in Release 12.1(4)E1, page 102
- New Software Features in Release 12.1(4)E1, page 102

New Hardware Features in Release 12.1(4)E1

None.

New Software Features in Release 12.1(4)E1

None.

Note Support for mobile IP, introduced in Release 12.1(2)E, was inadvertently deleted from Release 12.1(4)E1, Release 12.1(3a)E4, and Release 12.1(3a)E3 (see CSCds78103 in the "Open Caveats in Release 12.1(8b)E20" section on page 282).

New Features in Release 12.1(3a)E7

These sections describe the new features in Release 12.1(3a)E7, 15 Feb 2002:

- New Hardware Features in Release 12.1(3a)E7, page 102
- New Software Features in Release 12.1(3a)E7, page 102

New Hardware Features in Release 12.1(3a)E7

None.

New Software Features in Release 12.1(3a)E7

None.

New Features in Release 12.1(3a)E4

These sections describe the new features in Release 12.1(3a)E4, 24 Oct 2000:

- New Hardware Features in Release 12.1(3a)E4, page 103
- New Software Features in Release 12.1(3a)E4, page 103

New Hardware Features in Release 12.1(3a)E4

None.

New Software Features in Release 12.1(3a)E4

None.

New Features in Release 12.1(3a)E3

These sections describe the new features in Release 12.1(3a)E3, 10 Oct 2000:

- New Hardware Features in Release 12.1(3a)E3, page 103
- New Software Features in Release 12.1(3a)E3, page 103

New Hardware Features in Release 12.1(3a)E3

None.

New Software Features in Release 12.1(3a)E3

Release 12.1(3a)E3 supports the following new software features:

- Cisco IOS server load balancing (Cisco IOS SLB) enhancements:
  - Ping probes
  - Firewall Load Balancing

  Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e3/iosslb3.htm
- For the following features, refer to these publications:
  - The *Catalyst 6500 Series Cisco IOS Software Configuration Guide* at this URL:

    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/index.htm
  - The *Catalyst 6500 Series Cisco IOS Command Reference* publication at this URL:

    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/index.htm
- Redundant configuration enhancement—The **show module** command displays supervisor engine redundancy status.

- IP MMLS global threshold—Refer to the "Configuring IP Multicast Layer 3 Switching" chapter of the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and to the *Catalyst 6500 Series Cisco IOS Command Reference* publication.
- Aggressive UniDirectional Link Detection (UDLD)—Refer to the "Configuring UDLD" chapter of the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and to the *Catalyst 6500 Series Cisco IOS Command Reference* publication.
- Router-Port Group Management Protocol (RGMP)—Refer to the "Configuring RGMP" chapter of the *Catalyst 6500 Series Cisco IOS Software Configuration Guide*.
- Spanning Tree Protocol (STP) 32-bit path cost feature—Refer to the "Configuring STP" chapter of the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and to the *Catalyst 6500 Series Cisco IOS Command Reference* publication.
- Spanning Tree Protocol Root Guard Feature—Refer to the "Configuring STP Features" chapter of the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and to the *Catalyst 6500 Series Cisco IOS Command Reference* publication.

Note To support the requirements of future hardware, the maximum value of the **interface port-channel channel-group** command has been reduced to 64.

New Features in Release 12.1(2)E2

These sections describe the new features in Release 12.1(2)E2, 14 Feb 2002:

- New Hardware Features in Release 12.1(2)E2, page 104
- New Software Features in Release 12.1(2)E2, page 104

New Hardware Features in Release 12.1(2)E2

None.

New Software Features in Release 12.1(2)E2

None.

New Features in Release 12.1(2)E

These sections describe the new features in Release 12.1(2)E, 26 Jun 2000:

- New Hardware Features in Release 12.1(2)E, page 104
- New Software Features in Release 12.1(2)E, page 105

New Hardware Features in Release 12.1(2)E

Release 12.1(2)E provides initial support for these products:

- WS-C6509-NEB—Catalyst 6509-NEB chassis (9 vertical slots)
- WS-F6K-MSFC2—MSFC2 router daughter card

- WS-X6416-GBIC—16-port Gigabit GBIC Ethernet switching module
- WS-6316-GE-TX—16-port Gigabit Ethernet RJ-45 switching module
- WS-X6348-RJ-45—48-port 10/100TX RJ-45 Ethernet switching module with 128 KB per-port packet buffers
- WS-X6324-100FX—24-port 100FX Ethernet switching module with 128 KB per-port packet buffers

New Software Features in Release 12.1(2)E

Release 12.1(2)E supports the following new software features:

- Mobile IP—Refer to the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1, "Configuring Mobile IP," at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdmobip.htm

- Web Cache Control Protocol (WCCP) Layer 2 PFC redirection—WCCP Layer 2 PFC redirection allows directly connected Cisco Cache Engines to use Layer 2 redirection, which is more efficient than Layer 3 redirection with generic route encapsulation (GRE). A directly connected Cache Engine can be configured to negotiate use of the WCCP Layer 2 PFC Redirection feature. The WCCP Layer 2 PFC redirection feature requires no configuration on the MSFC. The **show ip wccp web-cache detail** command displays which redirection method is in use for each cache. Observe the following guidelines:
  - The WCCP Layer 2 PFC redirection feature sets the IP flow mask to full-flow mode.
  - You can configure the Cisco Cache Engine software release 2.2 or later to use the WCCP Layer 2 PFC redirection feature.
  - Layer 2 redirection takes place on the switch and is not visible to the MSFC. The **show ip wccp web-cache detail** command on the MSFC displays statistics for only the first packet of a Layer 2 redirected flow, which provides an indication of how many flows, rather than packets, are using Layer 2 redirection. Entering the **show mls entries** command on the supervisor engine displays the other packets in the Layer 2 redirected flows.

  Configure the Cisco IOS WCCP as described in the *Cisco IOS Configuration Fundamentals Configuration Guide*, under "Configuring Web Cache Services Using WCCP," at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd305.htm

- Cisco IOS server load balancing (Cisco IOS SLB) enhancements:
  - Client NAT
  - HTTP probe
  - Stateful backup
  - CISCO-SLB-MIB support

  Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/iosslb2.htm

- For the following features, refer to these publications:
  - The *Catalyst 6500 Series Cisco IOS Software Configuration Guide* at this URL:

    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/index.htm
  - The *Catalyst 6500 Series Cisco IOS Command Reference* publication at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/index.htm

- UniDirectional Link Detection—Refer to the "Configuring UDLD" chapter of the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and to the *Catalyst 6500 Series Cisco IOS Command Reference* publication.
- Local proxy ARP—Refer to the *Catalyst 6500 Series Cisco IOS Command Reference* publication for information about the **ip local-proxy-arp** command.

Note To use the local proxy ARP feature, you must enable the IP proxy ARP feature. The IP proxy ARP feature is enabled by default. Refer to the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1, "IP Addressing and Services," "Configuring IP Addressing," "Enabling Proxy ARP," at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdipadr.htm

New Features in Release 12.1(1)E6

These sections describe the new features in Release 12.1(1)E6, 17 Feb 2002:

- New Hardware Features in Release 12.1(1)E6, page 106
- New Software Features in Release 12.1(1)E6, page 106

New Hardware Features in Release 12.1(1)E6

None.

New Software Features in Release 12.1(1)E6

None.

New Features in Release 12.1(1)E2

These sections describe the new features in Release 12.1(1)E2, 20 Feb 2000:

- New Hardware Features in Release 12.1(1)E2, page 106
- New Software Features in Release 12.1(1)E2, page 106

New Hardware Features in Release 12.1(1)E2

None.

New Software Features in Release 12.1(1)E2

None.

New Features in Release 12.1(1)E

These sections describe the new features in Release 12.1(1)E:

- New Hardware Features in Release 12.1(1)E, page 107
- New Software Features in Release 12.1(1)E, page 107

New Hardware Features in Release 12.1(1)E

None.

New Software Features in Release 12.1(1)E

Release 12.1(1)E supports these new software features:

- Quality of service (QoS) supports IPX and MAC-layer traffic, in addition to IP traffic. Refer to these publications:
  - The "Configuring QoS" chapter in the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* at this URL:

    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/index.htm
  - The *Catalyst 6500 Series Cisco IOS Command Reference* publication at this URL:

    http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/index.htm
- Cisco IOS server load balancing (Cisco IOS SLB) enhancements are as follows:
  - Server Network Address Translation (NAT)
  - Cisco IOS SLB stateless redundancy

  Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e1/iosslb1.htm
- Support for the CISCO-L2L3-INTERFACE-CONFIG-MIB

New Features in Earlier Releases

These sections describe the new features in earlier releases:

- New Hardware Features in Earlier Releases, page 107
- New Software Features in Earlier Releases, page 107

New Hardware Features in Earlier Releases

Release 12.0 XE provides initial support of the Cisco IOS for the Catalyst 6000 Family Switches product, which runs Cisco IOS software on both the Supervisor Engine 1 and the MSFC.

New Software Features in Earlier Releases

Release 12.0 XE provides initial support of the Cisco IOS for the Catalyst 6000 Family Switches product, which runs Cisco IOS software on both the Supervisor Engine 1 and the MSFC1.

- The Layer 2 features are as follows:

  Note The following chapter references are to the *Catalyst 6500 Series Cisco IOS Software Configuration Guide*.

  - Layer 2 switch ports and VLAN trunks with the Dynamic Trunking Protocol (DTP), including support on Gigabit Ethernet ports for jumbo frames (refer to the "Configuring Layer 2 Ethernet Interfaces" chapter)
  - VLANs (refer to the "Configuring VLANs" chapter)
  - VLAN Trunk Protocol (VTP) and VTP domains (refer to the "Configuring VTP" chapter)
  - Spanning Tree Protocol (refer to the "Configuring STP" chapter)
  - Spanning tree PortFast, UplinkFast, and BackboneFast (refer to the "Configuring STP Features" chapter)
  - IGMP snooping (refer to the "Configuring IGMP Snooping" chapter)
  - Broadcast Suppression (refer to the "Configuring Broadcast Suppression" chapter)
- The Layer 3 features are as follows:
  - Layer 3 routing protocols (refer to the Cisco IOS *Network Protocols Configuration Guides*, Parts 1 and 2, and the Cisco IOS *Network Protocols Command Reference* publication, Parts 1 and 2):

    Static IP routing
    IP routing protocols
    IP multicast routing protocols
    IPX routing protocols
    Apollo
    AppleTalk Routing
    DECnet
    VINES
    XNS
  - Layer-3 related protocols (refer to the Cisco IOS Release 12.1 *Network Protocols Configuration Guides*, Parts 1 and 2, and the Cisco IOS Release 12.1 *Network Protocols Command Reference* publication, Parts 1 and 2):

    Internet Group Management Protocol (IGMP) v1 and v2
    Cisco Group Multicast Protocol (CGMP) server support
    Full Internet Control Message Protocol (ICMP) support
    Gateway Discovery Protocol (GDP)
    ICMP Router Discovery Protocol (IRDP)
    Multicast Source Discovery Protocol (MSDP)
    Multicast Border Gateway Protocol (MBGP)
  - Jumbo frame support on Gigabit Ethernet ports (refer to the "Configuring Layer 3 Ethernet Interfaces" chapter)
- Data-link switching plus (DLSw+)
- WCCP, versions 1 and 2

- These services are supported in this release:
  - Standard Domain Naming System (DNS) support (refer to the Cisco IOS *Network Protocols Configuration Guide*, Part 1, and the Cisco IOS *Network Protocols Command Reference* publication, Part 1)
  - Dynamic Host Configuration Protocol (DHCP); (refer to Cisco IOS *IP and IP Routing Configuration Guide*, Release 12.1, "Configuring DHCP")
  - Boot Protocol (BOOTP) relay (refer to the Cisco IOS *Network Protocols Configuration Guide*, Part 1, and the Cisco IOS *Network Protocols Command Reference* publication, Part 1)
  - Multiple-Hot Standby Routing Protocol (M-HSRP; refer to "Hot Standby Router Protocol" in the Cisco IOS *Network Protocols Configuration Guide*, Part 1, and the Cisco IOS *Network Protocols Command Reference* publication, Part 1)
  - Cisco Discovery Protocol (CDP); (refer to the "Configuring CDP" chapter)
  - Standard IP access control lists (ACLs) at wire rate (refer to the "Configuring Network Security" chapter)
  - Standard reflexive ACLs (refer to the "Configuring Network Security" chapter)
  - NetFlow Data Export (refer to the "Configuring NDE" chapter)
  - Access control using several supported authentication methods (refer to the "Configuring the Supervisor Engine" chapter)
  - Switched Port Analyzer (SPAN); (refer to the "Configuring SPAN" chapter)
  - Redundant supervisor engines (refer to the "Configuring the Supervisor Engine" chapter)
  - Quality of Service (QoS); (refer to the "Configuring QoS" chapter)
- Cisco IOS server load balancing (Cisco IOS SLB)—Refer to this online publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e1/iosslb1.htm

Note Web Cache Control Protocol (WCCP) Layer 2 PFC redirection is supported with Cisco IOS SLB SLB. Other WCCP configurations are not compatible with Cisco IOS SLB.

Features Not Supported

- Hardware—See the "Unsupported Hardware" section on page 28
- High availability
- Ability to accept ingress traffic on SPAN destination ports (**set span ... inpkts enable**)
- Commands to globally disable EtherChannel or trunking
- Layer 2 traceroute
- **write tech-support** command
- **set port host** command
- Disable port startup option
- Diagnostic options on bootup with Supervisor Engine 1
- Clear counters per port or clear QoS statistics

- System warning and error counter enhancements implemented in Catalyst software release 6.1(1)
- Switch TopN reports
- Option for no VTP support
- Command to display the port MAC address
- Port security timer enhancement
- System warnings on port counters
- VLAN Management Policy Server (VMPS) client or server
- MAC-layer Cisco IOS access control lists (ACLs)
- Accelerated server load balancing (ASLB); Cisco IOS SLB is supported
- Hot Standby Router Protocol (HSRP) between redundant supervisor engines (the redundant supervisor engine and MSFC are in standby mode—HSRP to external routers is supported)
- Multi-Instance Spanning Tree Protocol (MISTP); IEEE 802.1s MST is supported
- Common Open Policy Server (COPS)
- Resource ReSerVation Protocol (RSVP)
- GARP VLAN Registration Protocol (GVRP)
- GARP Multicast Registration Protocol (GMRP)

Limitations and Restrictions

These sections list limitations and restrictions for Cisco IOS software for the Catalyst 6500 series switches and Cisco 7600 Series Routers:

- General Limitations and Restrictions, page 110
- FlexWAN Limitations and Restrictions, page 117
- OSM Limitations and Restrictions, page 118
- Service Module Limitations and Restrictions, page 118

Refer to the following site for information about MIBs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

General Limitations and Restrictions

This section describes general limitations and restrictions:

- When a redundant supervisor engine is in standby mode, the Ethernet ports on the redundant supervisor engine are always active.
- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannel (maximum of eight interfaces) with no requirement that the ports be contiguous.
- All Ethernet ports on all modules support 802.1Q VLAN trunking.

- These modules do not support Inter-Switch Link (ISL) VLAN trunking:
  - WS-X6502-10GE
  - WS-X6548-GE-TX
  - WS-X6148-GE-TX
- The link state messages ("LINK-3-UPDOWN" and "LINEPROTO-5-UPDOWN") are disabled by default. With Release 12.1(19)E1a and later releases, enter the **logging event link status** command on each interface where you want the messages enabled.
- In Release 12.1(19)E and later releases, you cannot disable IP routing. (CSCdu05871)
- IPsec in software on the MSFC is supported only for administrative connections to Catalyst 6500 series switches and Cisco 7600 series routers.
- SPAN and RSPAN destination ports and VACL capture ports can receive VACL-redirected traffic. (CSCea57673)
- If you have a network device in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

  When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction enabled, a switch bridge ID (used by the spanning-tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

  If another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could win root bridge ownership because of the finer granularity in the selection of its bridge ID.
- Enter the **copy running-config startup-config** command and the **redundancy reload peer** command to synchronize SNMP ifIndexes when RPR+ redundancy and SNMP ifIndex persistence are configured when all modules are online after any system boot or when you insert a module while the system is running. (CSCdy16763)
- RPR+ redundancy automatic startup configuration synchronization supports only the nvram:startup-config file. With RPR+ redundancy configured, if you enter a **boot config** command that does not specify nvram:startup-config as the startup configuration file, you must manually copy the startup configuration file to the redundant supervisor engine's device specified in the boot config command. (CSCdx25320)
- RPR+ redundancy does not support configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- The following Supervisor Engine 1 software images exceed the 16 MB Supervisor Engine 1 bootflash size:
  - c6sup12-jk2o3sv-mz
  - c6sup12-pk2o3sv-mz
  - c6sup12-jk2sv-mz
  - c6sup12-jo3sv-mz
  - c6sup12-jsv-mz
  - c6sup11-jsv-mz
  - c6sup11-jk2sv-mz

Workaround: Use a Flash PC card in slot0 to run these images and make sure there is at least 1 MB free on the supervisor engine bootflash in case the system needs to save crash information. (CSCdx48936)

- Traffic flow and SNMP connectivity is interrupted briefly if you perform an online insertion and removal (OIR) that changes the number of fabric-enabled modules so that the switch must use a different fabric channel switching mode. (CSCdx39882)
- The Ethernet port ASICs drop frames that are invalid (for example, frames that are shorter than the minimum valid length). The Ethernet port ASICs do not keep a count of dropped frames. (CSCdx14209)
- With Erasable Programmable Logic Device (EPLD) versions 0006 or earlier versions and Release 12.1(8a)EX (and later 12.1 EX releases) or Release 12.1(11b)E (and later 12.1 E releases), all CoS values for the Gigabit Ethernet ports on the Supervisor Engine 2 are mapped to queue 1, threshold 1, by default and cannot be reconfigured. You cannot enter the following commands for the Gigabit Ethernet Ports on the Supervisor Engine 2:
  - wrr-queue cos-map
  - rcv-queue cos-map
  - priority-queue cos-map

  This affects only the Gigabit Ethernet ports on the Supervisor Engine 2. It does not any affect other ports on any other modules.

  Workaround: Upgrade the EPLD. Contact the TAC for more information. (CSCdw89764)
- With Release 12.1(12c)E1 and later releases, you can enter the **no mls qos channel-consistency** command to support an EtherChannel with QoS enabled that has interfaces with and without strict-priority queues. In earlier releases, when you enable QoS, interfaces drop out of any EtherChannels that contain both interface types.
- With a PFC2:
  - Any options in Cisco IOS ACLs that provide filtering in a policy-map class that would cause flows to be sent to the MSFC2 to be switched in software are ignored. For example, logging is not supported in ACEs in Cisco IOS ACLs that provide filtering in QoS policy-map classes.
  - The PFC2 does not provide QoS for flows that match an ACE in a Cisco IOS ACL configured with options that cause the flows to be sent to the MSFC2 to be switched in software, except when the Cisco IOS ACL provides filtering in a QoS policy-map class. For example, the PFC2 does not provide QoS for flows that match an ACE in a Cisco IOS ACL with logging configured.

  (CSCds72804)
- For multicast flows, the PFC does not provide Layer 3 switching on output interfaces with MTU sizes smaller than the flow's input interface MTU size.

  Workaround: Configure the same MTU size on both the input and output interfaces. (CSCds42685)
- Entering the **clear mls qos** command affects the policing token bucket counters and might briefly allow traffic to be forwarded, which would otherwise be policed. (CSCdt40470)
- With a PFC2 and DFCs, you cannot attach QoS policies to VLANs; do not enter the **mls qos vlan-based** command.
- The **mls qos vlan-based** command configures all interfaces on switching modules with **1p1q0t/1p3q1t** QoS port architecture.

- Integrated routing and bridging (IRB) and concurrent routing and bridging (CRB) have deliberately been disabled on the Catalyst 6500 series switches and Cisco 7600 Series Routers. You should use routable Layer 2 VLANs and VLAN interfaces for normal bridging and interVLAN routing. Bridge groups are supported only to bridge nonrouted protocols.
- With Release 12.1(6)E or later, FlexWAN module interfaces support dNBAR. Do not configure NBAR on other interfaces.
- Catalyst 6500 series switches and Cisco 7600 Series Routers do not support remote source-route bridging (RSRB).
- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannel (maximum of eight interfaces) with no requirement that interfaces be contiguous.
- With a PFC2 and DFCs, QoS ignores policy maps attached to an EtherChannel formed from interfaces on different DFC-equipped switching modules.
- To avoid a reload with redundant Switch Fabric Modules, if you perform any of these operations on the active Switch Fabric Module, wait at least 15 seconds before you perform any of these operations on the other Switch Fabric Module:
  - Removing the Switch Fabric Module
  - Inserting the Switch Fabric Module
  - Entering commands to power cycle the Switch Fabric Module
  - Entering commands to power down the Switch Fabric Module
  - Entering commands to power up the Switch Fabric Module

  (CSCdt43548)
- Ingress IP Packets with TTL=1 that are not addressed to the MSFC2 and that match QoS filtering parameters might cause overpolicing of other ingress traffic on the same ingress interface.
- With PFC2 (and DFCs, if present), the hardware FIB supports 256K entries, which includes 16K IP multicast entries. With RPF check enabled, there are twice as many IP entries in the FIB.
- With PFC2 (and DFCs, if present), hardware CEF-switching uses per-flow load balancing, based on IP source and destination addresses. For any given packet, all PFC2- and DFC-equipped switches make exactly the same load-balancing decision, which can result in nonrandom load balancing.
- When the outgoing interface list for group G traffic transitions to null on a last-hop multicast router, the router sends a (*,G) prune message to the PIM neighbor toward the rendezvous point (RP) to stop the flow of group G traffic (if any) down the shared tree, but does not send an (S,G) prune message to stop the flow of traffic down the shortest path tree (SPT). The transition of the outgoing interface list to null does not trigger an (S,G) prune message. (S,G) prune messages are triggered by the arrival of (S,G) traffic.

  If the last-hop multicast router is a Catalyst 6500 series switch, traffic is forwarded by the PFC2. In most cases, RPF-MFD is installed for the (S,G) entries. The MSFC2 does not see the multicast traffic flowing down the SPT and does not send any traffic-triggered (S,G) prunes to stop the flow of traffic down the SPT. This situation does not have any adverse effect on the MSFC2 because the PFC2 processes and drops the unwanted (S,G) traffic.
- With a PFC2, if you enter the **mac** *mac_address* interface command, the configured MAC address is used for all Layer 3 VLAN interfaces and Layer 3 LAN ports.
- The PFC2 supports a maximum of 1 Gateway Load Balancing Protocol (GLBP) group.
- The PFC2 supports a maximum of 16 unique Hot Standby Routing Protocol (HSRP) group numbers.
  - You can use the same HSRP group numbers in different VLANs (for example, use 1 as the first group number in each VLAN, 2 for the second, etc.).

  - If you configure more than 16 HSRP groups, this restriction prevents use of the VLAN number as the HSRP group number.

- A Supervisor Engine 1 must have ROMMON version 5.2(1) or later.
- You must have a boot loader image in an MSFC1 bootflash device to boot successfully. Do not reset the switch when there is no boot loader image in the MSFC1 bootflash device. If there is no boot loader image in the MSFC1 bootflash device and the state of the switch does not support the **copy** command, see the "Recovering From Loss of the Boot Loader Image" section on page 320.
- The **ip multicast rate-limit** command is not supported on Catalyst 6500 series switch LAN ports. For information about policing, refer to the online *Catalyst 6500 Series Cisco IOS QoS Configuration Guide* at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/ios127xe/qos.htm

  (CSCds22281)
- Catalyst 6500 series switches and Cisco 7600 Series Routers do not support network booting.
- You can specify a Catalyst 6500 series switch or Cisco 7600 series router as the MLS route processor (MLS-RP) for Catalyst 5000 family switches using MLS. Refer to the *Layer 3 Switching Configuration Guide—Catalyst 5000 Family, 4000 Family, 2926G Series, 2926 Series, 2948G* for MLS configuration procedures.
- The IP HTTP server feature is disabled by default. Enter the **ip http server** command to use the feature.
- For LAN switching modules, the Cisco IOS **show controllers** command generates no output on a Catalyst 6500 series switch or Cisco 7600 series router. Enter the **show module** command instead.
- To avoid the case where all traffic is out of profile, the burst size specified in a QoS policing rule must be at least as large as the maximum packet size permissible in the traffic to which the rule is applied.
- When using the NAT router feature on a Catalyst 6500 series switch, packets traversing the NAT outside interface might in certain configurations be software routed instead of Layer 3 switched, regardless of whether they should or should not be translated. For packets traversing the NAT outside interface, only those packets requiring NAT should be software routed. Cisco IOS only translates traffic that is traversing from NAT inside interfaces to NAT outside interfaces and vice versa.

  Make the ACL used for NAT more specific to limit the software-handled packets to only those packets requiring NAT translation. For example, if you use a general ACL (such as **permit ip any any**) to specify the traffic that requires NAT, then all traffic inbound or outbound on the NAT outside interface will be software routed (including traffic not originating or destined to the NAT inside interfaces). If it is possible to use a more specific ACL (such as **permit ip 10.1.1.0 0.0.0.255 any**), then only the NAT outside traffic matching that ACL will be software routed. This traffic will still be software routed regardless of whether it is originating from or destined to NAT inside interfaces. However, by making the ACL more specific, you can limit the amount of traffic that is software routed due to the NAT ACL.
- By default, the MSFC sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group.

  With the **ip unreachables** command enabled (which is the default), the Supervisor Engine 2 drops most of the denied packets in hardware and sends only a small number of packets (10 packets per second, maximum) to the MSFC2 to be dropped, which generates ICMP-unreachable messages.

  With the **ip unreachables** command enabled, the Supervisor Engine 1 sends all the denied packets to the MSFC to be dropped, which generates ICMP-unreachable messages.

To eliminate the load imposed on the MSFC CPU by the task of dropping denied packets and generating ICMP-unreachable messages, do the following:

  - With Supervisor Engine 1, enter the **no ip unreachables** interface configuration command.
  - With Supervisor Engine 2, enter the **no ip unreachables** and the **no ip redirects** interface configuration commands. (CSCdr33918)

- MAC address-based Cisco IOS ACLs are not supported for packets that are Layer 3 switched in hardware. MAC address-based Cisco IOS ACLs will be applied on software-switched packets.
- If you enable multicast routing globally, then you should also enable multicast routing (using the **ip pim** command) on all Layer 3 interfaces on which you anticipate receiving IP multicast traffic. This command causes the packets to be sent to the process switching level to create the route entry. If you disable multicast routing on the RPF interface, the entry cannot be created and the packet is dropped. If the source traffic rate exceeds what can be handled by the process level, it can have an undesirable impact on the system. For example, routing protocol packets, such as EIGRP hello packets, might get dropped.
- 24-port 100FX switching modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower only support IEEE 802.1Q VLAN trunking; they do not support ISL trunking. Do not configure ISL trunks on 24-port 100FX switching modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower. The restriction against ISL VLAN trunking is the only known problem with hardware version 1.1 or lower of these modules. If you do not require ISL VLAN trunking, these modules are fully functional. The ISL VLAN trunking problem has been corrected in hardware version 1.2 or later. If you want to return a WS-X6224-100FX-MT module with a hardware version of 1.1 or lower, contact Cisco Systems. You can identify WS-X6224-100FX-MT hardware versions using one of these two methods:
  - Command-line interface (CLI) method—Enter the **show module** command to identify the hardware version of the WS-X6224-100FX-MT module.
  - Physical inspection method—The part number is printed on a label on the outer edge of the component side of the module. Versions 73-3245-04 or lower do not support ISL trunking.
- The RJ-21 connectors on the 48-port 10/100TX switching module (WS-X6248-TEL) do not support Category 3 RJ-21 telco connectors and cabling. Category 3 connectors and cabling cause carrier sense errors. Use Category 5 RJ-21 telco connectors and cables (the module is keyed for Category 5 telco connectors and cables).
- The in and out ports displayed in Layer 3 table entries are set by the hardware at the time the entry is created. They are not guaranteed to be accurate in case multiple flows use the same entry (for example, if the flow mask is **Dest-only** and some kind of load sharing is active) or if the source or destination of the Layer 3 entry moves in the Layer 2 topology. The port information is not always available when the Layer 3 entry is established. This is the case if the destination port of the rewritten packet is unknown when the shortcut is created.
- NetFlow Data Export (NDE) version 7 is not supported for MLS statistics exported from the MSFC. NDE on the PFC supports the following NDE versions to export the statistics captured on the PFC for Layer 3-switched traffic:
  - Supervisor Engine 1 and PFC—NDE version 7
  - Supervisor Engine 2 and PFC2:

    NDE version 5 with Release 12.1(13)E and later releases

    NDE version 7 with all releases
- For EtherChannels, you can configure the QoS trust state and default CoS directly on the EtherChannel interface with the **mls qos trust** or **mls qos cos** commands, respectively. These two parameters must be the same for all physical interfaces in the channel. No other QoS queueing

configuration commands can be applied to EtherChannel interfaces. Other QoS queueing configuration commands can be applied, however, to individual EtherChannel physical interfaces. After the physical interfaces are bundled into an EtherChannel, QoS classification, marking, and policing by the Policy Feature Card (PFC) for the channel packets is determined by the service-policy attached to the EtherChannel interface. The service policies attached to the individual physical interfaces of the EtherChannel do not matter. The same is true for the port-based and VLAN-based QoS state of the EtherChannel interface. You can disable the PFC QoS features using the **no mls qos** interface configuration command on the EtherChannel interface.

- Cisco IOS running on the supervisor engine and the MSFC does not support the IEEE bridging protocol for bridge groups. You should configure bridge groups to use VLAN-bridge or DEC protocol spanning tree.
- The maximum recommended number of Layer 3 multicast entries is 10,000. The maximum recommended number of multicast entries supported in the Layer 2 forwarding table is 12,000.
- After enabling Protocol Independent Multicast (PIM) on an interface, you need to enter the **ip mroute-cache** command on the interface to enable multicast fast-switching. If you have "no ip mroute-cache" configured, multicast packets that are not hardware switched will go to the process level that increases the load on the router.
- The **show ibc** command misleadingly displays Inter-Switch Link (ISL) trunk status as "disabled" and the GBIC as "missing," because the IBC in a Catalyst 6500 series switch or Cisco 7600 series router is the internal electrical interface between the switch processor and the route processor. Trunk and media types are not given for this type of interface. (CSCdp21121, CSCdp21380)
- With Supervisor Engine 1 and PFC, when you upgrade from Release 12.1(2)E to 12.1(3a)E2, it is safe to ignore "ip cef incomplete command" error messages. (CSCds43045)
- The **show access-list** command displays statistics only for traffic that matches ACLs processed in software on the MSFC. The **show access-list** command does not display statistics for traffic that matches an ACL supported in hardware on the PFC. (CSCdt14386)
- The **show interface stats** command does not display statistics for traffic that is Layer 3 switched by the PFC. The **show interface** command displays statistics (labelled **L2** and **L3**) for traffic that is Layer 3 switched by the PFC2. (CSCds41388)
- To avoid subjecting routing protocol packets to policy-based routing, configure filtering in route maps so that it does not match routing protocol packets. (CSCds44369)
- Microflow policing does not support policing of identical flows arriving on different interfaces simultaneously. Attempts to do so lead to incorrectly policed flows. (CSCdt72147)
- Because the system does not boot from MSFC bootflash, if the NVRAM configuration is not valid (or not present), the **service config** option defaults to "on," and the service config feature is enabled after the **erase startup-config** command is issued. (CSCdp12598)
- In a VTP version 1 domain with some switches running Catalyst software and some switches running Cisco IOS software on both the supervisor engine and the MSFC, if the VLANs were created on a switch running Catalyst software and then propagated through VTP to switches running Cisco IOS software, if you enter commands on the switches running Cisco IOS software to configure VTP version 2, you might receive messages about invalid VLAN configuration.

  Workaround: Perform VLAN configuration on a switch running Catalyst software or enter VLAN configuration commands to correct all VLAN configuration errors reported in the messages. (CSCdp47622)
- When you upgrade to a later software release, WS-X6816-GBIC switching modules might reset more than once when the new release boots for the first time. (CSCdw87069)

- The **interface range** command is not supported by the HTTP user interface. The command will execute on only the first interface in the specified range. Do not use the **interface range** command with the HTTP interface. (CSCdm54471)
- Supervisor Engine 2 and Supervisor Engine 1 typically are able to learn at least 32 K MAC addresses.
- When you boot Release 12.1(13)E1 dsv images, the following messages are displayed:

```
00:01:15: %PPP-4-NOREGISTER: NCP not registered, protocol = 0
00:01:15: %PPP-4-NOREGISTER: NCP not registered, protocol = 0
00:01:15: %PPP-4-NOREGISTER: NCP not registered, protocol = 0
00:01:15: %PPP-4-NOREGISTER: NCP not registered, protocol = 0
00:01:15: %PPP-4-NOREGISTER: NCP not registered, protocol = 0
00:01:15: %PPP-4-NOREGISTER: NCP not registered, protocol = 0
```

  These messages are informational only. (CSCdy38295)
- With Release 12.1(11b)EX and earlier releases, a redundant Supervisor Engine 1 might fail to boot following a reload.

  Workaround: Enter the **no power enable module** *redundant_slot* and **power enable module** *redundant_slot* commands. (CSCec07946)
- Fast-switched IP multicast traffic is dropped when it matches a permit access list entry configured with the **log** keyword. Fast switching of IP multicast packets is enabled by default. (CSCds28581)
- When using the UplinkFast feature, the system does not send out the dummy multicast packets used to notify upstream users of forwarding-path changes. The system uses normal Layer 2 aging to delete invalid entries. (CSCdm65881)
- A MAC address that moves from a secure port to a nonsecure port and back to a secure port might cause high Supervisor Engine CPU utilization.

  Workaround: Clear the MAC address entry from the MAC address table. Enable port security on all ports where MAC address moves are common. (CSCin56672)
- If the MSFC address falls within the range of a PBR ACL, traffic addressed to the MSFC is policy routed in hardware instead of being forwarded to the MSFC. To prevent policy routing of traffic addressed to the MSFC, configure PBR ACLs to deny traffic addressed to the MSFC. (CSCse86399)

FlexWAN Limitations and Restrictions

- On FlexWAN ports configured for EoMPLS, the counters displayed by the **show mpls** command for parallel links between LERs do not update. (CSCdw04208, CSCdu87648)
- On FlexWAN ports, an EoMPLS virtual circuit stays up when the VLAN interface is down. (CSCdv69982)
- Ethernet over Multiprotocol Label Switching (EoMPLS) per-VLAN traffic shaping does not work with a FlexWAN egress port. (CSCdx10583)
- On FlexWAN ports, an EoMPLS virtual circuit stays up when the VLAN interface is down. (CSCdv69982)
- To use the interfaces on the FlexWAN module, you must enable IP routing on the MSFC. (CSCdp34896)
- Support for MPLS and EoMPLS features on FlexWAN requires a Supervisor Engine 2 and MSFC 2.

OSM Limitations and Restrictions

- If you use the Class-Based Weighted Fair Queueing (CBWFQ) **shape average** command and apply the configured policy map to an interface on an OSM, traffic-shaping accuracy cannot be guaranteed if the target bit rate specified is less than 256,000 bits per second. (CSCea06515)
- For the OC-12 ATM OSM, the Common Part Convergence Sub-layer User-to-User (CPCS-UU) field in the AAL5 CPCS PDU cannot be set, cleared, or transported correctly. This affects custom use of the field as well as FRF8.1, which uses the CPCS-UU byte to transport the Frame Relay command response bit. This is a hardware issue that affects all releases. There is no workaround. (CSCeb36223)
- The PFC2 QoS **police** command and the PXF-based **set** command are both used to set IP precedence. However, when you configure the **set ip prec** command for an OSM VPN path, the **mls qos** command is ignored. (CSCdw83517)
- The Gigabit Ethernet WAN ports on the OSM-4GE-WAN-GBIC and OSM-2+4GE-WAN+ switching modules do not support traffic in the native VLAN of an IEEE 802.1Q trunk. Do not configure a subinterface with the **encapsulation dot1q** *vlan_id* **native** command. (CSCdx60011)
- When you upgrade from OSM-4GE-WAN-GBIC to an OSM-2+4GE-WAN+, the existing configuration will not be saved and applied to the new OSM-2+4GE-WAN+. To save your configuration when upgrading from an OSM-4GE-WAN-GBIC to an OSM-2+4GE-WAN+, perform this task:

  1. Enter the **write memory** command before removing the OSM-4GE-WAN-GBIC
  2. Install the new OSM-2+4GE-WAN+
  3. Enter the **copy startup-config running-config** command
  4. Enter the **write memory** command

  (CSCdz80308)
- When you apply the first policy map or remove the last policy map from an interface on an OSM-1OC48-POS-SS,-SI, -SL module traffic through the interface may be disrupted and the routing protocol may go up and down. (CSCdx94033)
- The channelized OSMs are not supported in the MPLS core. They support IP traffic on customer edge (CE) and provider edge (PE) router links only.
- Unless you enter the **mls qos** command to enable PFC QoS, when you enable MPLS and enter the **random-detect** command in the output policy map on an interface, all OSM traffic through the interface is marked with DSCP 0. (CSCdw79863)
- The OSMs are supported only in systems with a Supervisor Engine 2.
- If you enter an input **set** command to modify IP precedence for an IP-to-Tag path, the MPLS experimental bits will continue to be derived from the prior IP-precedence setting. In order to modify the experimental bits, use the **set mpls exp** command on the ingress interface. (CSCdw66785)

Service Module Limitations and Restrictions

- When the NAM is configured as the NDE destination and the NAM is down, the NDE traffic is flooded.

  Workaround: Clear the NDE configuration for the NAM or enter the **clear arp-cache** command. (CSCdy55261)

Caveats

These sections describe caveats:

- Release 12.1(27b)E and Rebuilds, page 119
- Release 12.1(26)E and Rebuilds, page 132
- Release 12.1(23)E and Rebuilds, page 159
- Release 12.1(22)E and Rebuilds, page 173
- Release 12.1(20)E and Rebuilds, page 192
- Release 12.1(19)E and Rebuilds, page 212
- Release 12.1(14)E, page 220
- Release 12.1(13)E and Rebuilds, page 226
- Release 12.1(12c)E and Rebuilds, page 262
- Release 12.1(11b)E and Rebuilds, page 270
- Release 12.1(8b)E and Rebuilds, page 281
- Release 12.1(7a)E and Rebuilds, page 303
- Release 12.1(6)E and Rebuilds, page 305
- Release 12.1(5c)E and Rebuilds, page 307
- Release 12.1(4)E1, page 313
- Release 12.1(3a)E Rebuilds, page 315
- Release 12.1(2)E and Rebuilds, page 317
- Release 12.1(1)E and Rebuilds, page 318

Note All caveats in Release 12.1 also apply to the corresponding 12.1E releases. Refer to the *Caveats for Cisco IOS Release 12.1* publication:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121relnt/121cavs/121mcavs.htm

Release 12.1(27b)E and Rebuilds

- General Caveats, page 120
- FlexWAN Caveats, page 129
- Service Module Caveats, page 130
- OSM Caveats, page 131

Note The caveat lists for Release 12.1(27b)E and rebuilds are updated frequently.

General Caveats

- Open General Caveats in Release 12.1(27b)E4, page 120
- Resolved General Caveats in Release 12.1(27b)E4, page 120
- Resolved General Caveats in Release 12.1(27b)E3, page 121
- Resolved General Caveats in Release 12.1(27b)E2, page 121
- Resolved General Caveats in Release 12.1(27b)E1, page 123
- Resolved General Caveats in Release 12.1(27b)E, page 125

Open General Caveats in Release 12.1(27b)E4

None.

Resolved General Caveats in Release 12.1(27b)E4

Resolved Caveats for Product 'all' and Component 'dlsw'

- CSCsk73104—Resolved in 12.1(27b)E4

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml

Resolved Caveats for Product 'all' and Component 'vpdn'

- CSCsj58566—Resolved in 12.1(27b)E4

  Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

  The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

  Cisco has made free software available to address these vulnerabilities for affected customers.

  There are no workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml

Identifier	Product	Component	Description
CSCsk26719	all	ip-acl	show ip access crash with per-user acl
CSCed52749	all	ospf	OSPF: route missing even though OSPF database still exists
CSCsg39295	all	snmp	Syslog Displays Password if SCP or FTP Selected in CISCO-COPY-CONFIG-MIB
CSCed95187	all	tcp	IP ID field is predictable for connectionless RST packets .
CSCsj64023	c7600	osm-ucode	MPLS: Sup2 OSM sending TTL=0 packets on MPLS VPN

Resolved General Caveats in Release 12.1(27b)E3

- CSCin95836—Resolved in Release 12.1(27b)E3.

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.
- Some UDP packets that have the Terminal Access Controller Access Control System (TACACS) port (49) as their destination might remain suspended in the interface queue. This problem occurs when TACACS+ is configured. This problem is resolved in Release 12.1(27b)E3. (CSCsb11698)
- A reload might occur when a frame relay sub-interface is deleted. This problem is resolved in Release 12.1(27b)E3. (CSCsi05251)
- Fast Ethernet port speed and duplex autonegotiaon might not work. This problem is resolved in Release 12.1(27b)E3. (CSCsi84306)

Resolved General Caveats in Release 12.1(27b)E2

- CSCsg70474—Resolved in Release 12.1(27b)E2

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml
- Closing a Telnet session may cause a reload. This problem is resolved in Release 12.1(27b)E2. (CSCds33629)

- In rare situations, intensive SNMP polling might use all available I/O memory. This problem is resolved in Release 12.1(27b)E2. (CSCeg11566)
- For a system configured as an IP HTTP server, tracebacks and a reload might occur during HTTP transactions with URL tokens greater than 128 characters long. A token is a string delimited by slashes in a URL. This problem is resolved in Release 12.1(27b)E2. (CSCeg62070)
- In certain LAN topologies, the PIM assert mechanism can cause an upstream router to erroneously remove downstream interfaces from output interface lists. When this situation occurs, it causes multicast traffic to be dropped. This problem occurs when two or more upstream routers with routes to the same rendezvous point or traffic source are connected to the same LAN segment as two different downstream routers. The problem occurs when the two downstream routers select different upstream routers as their next hop. This problem is resolved in Release 12.1(27b)E2. (CSCeh17756)
- A Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

  This problem is resolved in Release 12.1(27b)E2. (CSCsb12598, CSCsb40304, CSCsd92405)
- When a PBR route map is currently using an ACL, and then you modify, configure, or reapply the ACL, TCAM entries might be programmed incorrectly and cause a connectivity problem. This problem occurs when the ACL is on a Supervisor Engine 2. This problem is resolved in Release 12.1(27b)E2. (CSCse30376)
- A reload might occur when a routing event causes a Reverse Path Forwarding (RPF) interface to become an interface configured as a multicast boundary. This problem is resolved in Release 12.1(27b)E2. (CSCse92050)
- A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

There are workarounds available for this vulnerability.

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

This problem is resolved in Release 12.1(27b)E2. (CSCsf28840)

- A very slow memory leak might occur in the medium buffers. This problem occurs on a system configured with a distributed EtherChannel (DEC). When this problem occurs, MALLOCFAIL messages are displayed in the switch processor log. This problem is resolved in Release 12.1(27b)E2. (CSCsf31542)
- The WS-X6516A-GBIC and the WS-X6548-GE-TX switching modules might fail the TestL3VlanMet, TestIngressSpan and TestEgressSpan diagnostic tests when they come online while the system is in flow-through mode. This problem is resolved in Release 12.1(27b)E2. (CSCsg13124)
- This bug documents the deprecation and removal of the Cisco IOS FTP Server feature. This problem is resolved in Release 12.1(27b)E2. (CSCsg16908)
- On an MPLS VPN, when you use the BGP **aggregate-address** command with the **summary-only** keyword, all packets matching that aggregate will be sent out with TTL=0. This problem might also occur by redistributing an aggregate route into BGP. This problem is resolved in Release 12.1(27b)E2. (CSCsh21998)

Resolved General Caveats in Release 12.1(27b)E1

- CSCse68138—Resolved in Release 12.1(27b)E1.

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml
- The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

This problem is resolved in Release 12.1(27b)E1. (CSCek37177)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  This problem is resolved in Release 12.1(27b)E1 (CSCek26492)

- A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

  This problem is resolved in Release 12.1(27b)E1. (CSCsc64976)

- With the Cisco IOS Firewall CBAC feature enabled, if a client opens a connection to a server, which causes a firewall session to be created, and the connection is terminated on both the client and the server, the firewall session may never time out. This problem occurs with applications that use fixed source and destination ports. This problem is resolved in Release 12.1(27b)E1. (CSCsc72722)
- When establishing a DLSw Ethernet redundancy master and slave relationship, two devices never receive LLC frames transmitted one another. This problem is resolved in Release 12.1(27b)E1. (CSCsd55300)
- Port 2 or port 4 on a WS-X6816-GBIC switching module might go up and down when port 1 is enabled, not connected, and set to autonegotiate. This problem occurs if a 1000BASE-T GBIC was ever inserted since the last time the module was reloaded. This problem is resolved in Release 12.1(27b)E1. (CSCse12195)
- With DLSw Ethernet Redundancy configured, circuits might be established through the passive switch. This problem is resolved in Release 12.1(27b)E1. (CSCse17611)
- An enable authentication request might be sent erroneously to the AAA server group that was configured for login authentication. This problem is resolved in Release 12.1(27b)E1. (CSCsd95752)
- After a bridge group is removed, the bridge entry in a MAC nonaddress table might not be cleared for several minutes. This situation will result in a temporary interruption in fall-back bridging. This problem is resolved in Release 12.1(27b)E1. (CSCsc28959)

- With a tunnel configured to use an ATM interface, one end of the tunnel cannot ping the other end until you bring either end of the tunnel interface down and up. This problem is resolved in Release 12.1(27b)E1. (CSCse40423)
- Cisco IOS BGP is implemented with limits of 255 standard communities and 128 extended communities. RFC1771 Border Gateway Protocol 4 (BGP4) specifies that these communities should not be limited. This problem is resolved in Release 12.1(27b)E1. (CSCee30718)
- An "Unexpected Exception" and a reload might occur when you remove a switching module. This problem is resolved in Release 12.1(27b)E1. (CSCse55489)

Resolved General Caveats in Release 12.1(27b)E

- Symptoms: Router may generate and/or forward crafted IP packets with the source IP address being the routers tunnel interface for GRE or mGRE tunnels. Incorrect packet decoding may be seen with "debug tunnel."

  Conditions: The router needs to receive a specially crafted GRE packet sent to the tunnel end-point. The outer IP packet must come from the configured tunnel source and be sent to the configured tunnel destination IP address Present Routed bit must be set to 1.

  Workaround: Upgrade Cisco IOS to a version containing fixes for: CSCuk27655 or CSCea22552 or CSCei62762.

  Further information: On the 6th September 2006, Phenoelit Group posted an advisory:

  Cisco Systems IOS GRE decapsulation fault

  Cisco's statement and further information are available on the Cisco public website at:

  http://www.cisco.com/warp/public/707/cisco-sr-20060906-gre.shtml

  This problem is resolved in Release 12.1(27b)E. (CSCei62762)
- The **v2-single-tcp** keyword for the **dlsw remote-peer** command is not supported. Refer to this publication for more information about the keyword:

  http://www.cisco.com/en/US/tech/tk331/tk336/technologies_tech_note09186a0080093db6.shtml

  This problem is resolved in Release 12.1(27b)E. (CSCeb47150)
- The OSPF adjacencies in an area might reset if you enter the **area X stub** OSPF command or the **area Y nssa** OSPF command when the **area X stub** OSPF command or the **area Y nssa** OSPF command is already configured or if you enter a **copy startup-config running-config** command. This problem is resolved in Release 12.1(27b)E. (CSCec30212)
- Passwords and other sensitive information should not be sent to Access Control Server (ACS) logs. When command accounting is enabled, the full text of each command is sent to an ACS server. This information is sent to the server encrypted, but the server decrypts the packets and logs these commands in plain text. This problem is resolved in Release 12.1(27b)E. (CSCed09685)
- With a Supervisor Engine 720, you might see software-forced reloads. This problem is resolved in Release 12.1(27b)E. (CSCed36177)
- In releases where caveat CSCef46191 is resolved, attempts to open a Telnet connection may result in a "No Free TTYs" message even though many TTYs are available. This problem occurs after simultaneous Telnet requests. This problem is resolved in Release 12.1(27b)E. (CSCeg15044)
- If you enter the **ip forward-protocol turbo-flood** command, UDP broadcasts are not forwarded correctly on interfaces where bridge groups are configured. This problem is resolved in Release 12.1(27b)E. (CSCeg65640)

- Data Link Switching (DLSw) circuits might not connect using DLSw Ethernet redundancy. This problem occurs when DLSw Ethernet redundancy is configured with the following commands where the *local-mac* and *remote-mac* values are the same real MAC addresses of the remote host:
  - **dlsw transparent switch-support**
  - **dlsw transparent map local-mac** *local-mac*
  - **remote-mac** *remote-mac*

  If both DLSw routers are rebooted, clients can immediately establish a session with the remote host through one of these DLSw routers using the real MAC address. This real circuit is outside of Ethernet redundancy, and until the circuit is disconnected, Ethernet redundancy cannot be established. This problem is resolved in Release 12.1(27b)E. (CSCeh18295)
- DLSw load balancing using the circuit-count configuration does not distribute circuits evenly. This problem occurs when all the circuits attempt to connect at the same time. Configure the **dlsw load-balance round-robin** command initially, start DLSw, and then configure using **dlsw load-balance circuit-count**. This problem is resolved in Release 12.1(27b)E. (CSCeh18390)
- A system may lock for a long period of time while several instances of the following message are displayed:

  ```
  %CWAN_RP-4-SEMAHOG: Process 74 (MIP Mailbox)hogging CCB BLK Sema 10! calling proc 221
  (IFCOM Msg Hdlr)
  ```

  This problem is resolved in Release 12.1(27b)E. (CSCin79495)
- PPP packets are dropped while running software compression under heavy traffic. This problem is resolved in Release 12.1(27b)E. (CSCsa47223)
- Malformed VTP packets can cause a reload when debugging output is enabled for VLAN Trunk Protocol (VTP) events. This problem is resolved in Release 12.1(27b)E. (CSCsa82334)
- If a channel port receives a bridge protocol data unit (BPDU) message with an inconsistent VLAN ID from a neighbor, the supervisor engine successfully puts the port in a Port VLAN ID (PVID) inconsistent state but fails to block that port. The channel port could eventually move to the forwarding state due to an update in the STP topology. This situation occurs when the channel port is acting as a standby and is further blocked due to a PVID inconsistency. This situation could also occur if the inconsistency is not cleared. This problem is resolved in Release 12.1(27b)E. (CSCsb10031)
- When a Multiple Spanning Tree (MST) designated port receives a topology change (TC) from another MST region, it does not become a boundary port and it flushes only the internal spanning tree (IST) instance. This situation causes traffic loss in topologies that have VLANs mapped to instances other than the IST. This problem is resolved in Release 12.1(27b)E. (CSCsb79590)
- A standby supervisor engine in SSO mode might reload. This problem occurs when SNMP fills a data structure, and overwrites a byte of memory after the data structure. This problem is resolved in Release 12.1(27b)E. (CSCsc07793)
- When the *keep-exchanges* argument in the **frame-relay lmi-n391dte** command has a value that is lower than 3, Frame Relay autosensing does not function. This problem is resolved in Release 12.1(27b)E. (CSCea30197)
- When you enter the **eigrp log-event-type dual xmit transport** command and enable attributes and then enter the **show ip eigrp events** command to display the event log, a reload might occur . This problem is resolved in Release 12.1(27b)E. (CSCdx67130)
- A software-forced reload might occur after you configure and unconfigure Automatic Protection Switching (APS) revert. This problem is resolved in Release 12.1(27b)E. (CSCee91733)

- After you enter the **snmp-server enable traps sonet** command, the **no snmp-server enable traps sonet** command fails. If you enter the **show run** command, you will see that the traps are still enabled. This problem is resolved in Release 12.1(27b)E. (CSCeg41564)
- In RPR+ mode, when the standby supervisor engine is reset, an SNMP ModuleDown trap indicates that a specific module has been powered down or reloaded. The moduleType in this trap is 1 (other) instead of the correct value. This problem is resolved in Release 12.1(27b)E. (CSCeg81646)
- When you enter the **show mac** command for GBIC ports that are showing a notconnect status, you will see that the Out-Discard and Rcv-Octet counters continue to increment. This problem is resolved in Release 12.1(27b)E. (CSCeg64770)
- When you enter the **show controllers pos** *slot-number* **pm** *time-interval* command SONET statistics for POS interfaces are not displayed in the correct order in the output . The order of display should be the most recent first. This problem is resolved in Release 12.1(27b)E. (CSCea70822)
- The system might not allow incoming Telnet sessions. This problem occurs in a low-memory situation. This problem is resolved in Release 12.1(27b)E. (CSCdx39953)
- IOS Connectionless Network Service (CLNS) fast-switching is disabled on a serial E3 interface that is configured for High-Level Data Link Control (HDLC) encapsulation. This problem is resolved in Release 12.1(27b)E. (CSCsa45381)
- A system configured with DLSw+ Ethernet redundancy might reload when you enter the **show dlsw transparent neighbor** command. This problem is resolved in Release 12.1(27b)E. (CSCsc52939)
- A system configured for Point-to-Point Protocol (PPP) Multilink might reload because of a bus error. This problem is resolved in Release 12.1(27b)E. (CSCsa87205)
- A device might fail to start a DLSw session when the client sends an Exchange Identification (XID) to SSAP and DSAP populated with non-zero entries and without an ID block or number. The Logical Link Control (LLC) test frames indicate that the device never sees or acknowledges this XID frame to start the session. This problem is resolved in Release 12.1(27b)E. (CSCdy59779)
- If a Supervisor Engine 2 is configured with a Layer 2 nondistributed EtherChannel and a Layer 3 DEC, traffic ingressing on any port and egressing on the Layer 2 non-DEC, floods within the VLAN that contains the destination MAC address. This situation occurs when the EtherChannel purging timer expires (approximately every 21 minutes). The number of flooded packets depends on the traffic rate and Layer 2 table size. This problem is resolved in Release 12.1(27b)E. (CSCsc54382)
- A CPUHOG message might display when the system is configured with 200 multicast groups and processing traffic from 2000 hosts. This problem does not affect performance. This problem is resolved in Release 12.1(27b)E. (CSCdy64412)
- The output counters in the **show frame-relay pvc** *maplist* command are not being updated for either IP traffic or MPLS traffic. This problem is resolved in Release 12.1(27b)E. (CSCec08821)
- If OSPF is enabled on an interface, and then the configuration is changed to redistribute a connected route on this interface with a route map, then the route may not be redistributed correctly. This problem occurs only if the route map is used as a parameter with the **redistribute** command. This problem is resolved in Release 12.1(27b)E. (CSCee81606)
- In rare circumstances, a group of four ports (1 to 4, 5 to 8, 9- to 12, or 13 to 16) on the WS-X6516-GE-TX module may experience connectivity problems. If this problem occurs, the following syslog messages might be seen:

  ```
  %PM_SCP-SP-6-LCP_FW_ERR_INFORM: Module 4 is experiencing the following error:
  Pinnacle #0 Frames with Bad Packet CRC Error (PI_CI_S_PKTCRC_ERR - 0xC7) = 110
  ```

  This problem is resolved in Release 12.1(27b)E. (CSCef46923)

- Memory loss might occur with Web Cache Communication Protocol (WCCP) configured. This problem is resolved in Release 12.1(27b)E. (CSCeh79880)
- A system might require several attempts to initialize. If you set the diagnostics bootup level to bypass, the following message might be displayed:

  ```
  %SM-SP-4-BADEVENT: Event 'online' is invalid for the current state 'check_power_on'
  ```

  This problem is resolved in Release 12.1(27b)E. (CSCeh19437)
- When you enter the **mpls ip default-route** command, it is configured on the system and propogated to its Label Distribution Protocol (LDP) neighbors. If 0.0.0.0/0 is in the MPLS forwarding table and 0.0.0.0 in the routing table points towards one of the tag interfaces, any default route change will not be propagated to hardware forwarding tables. This problem is resolved in Release 12.1(27b)E. (CSCsa66067)
- If you enter the **show fm reflexive** command, and the number of reflexive flows exceeds one screen of display, the More prompt appears. The system might suspend if some of the reflexive flows that are not displayed yet are cleared before you attempt to display them. This problem is resolved in Release 12.1(27b)E. (CSCsa78258)
- A very large access control list (ACL) with many Layer 4 operators might allow some packets to pass through when using order-dependent ACL merge (ODM) optimizations. This problem occurs for packets that partially match a Layer 4 operator. This problem is resolved in Release 12.1(27b)E. (CSCsa79002)
- A system configured with Radius Load Balancing (RLB) reloads when you unconfigure a NAT server farm with connections. This problem is resolved in Release 12.1(27b)E. (CSCsa96560)
- If a static ARP entry is added to a configuration using the **arp** *ip-address mac-address* **arpa** command, then the entry cannot be deleted from the configuration when you use the **no arp** *ip-address mac-address* **arpa** command. This problem occurs when the address of the static entry that belongs to a subnet is configured on a routed interface as secondary. This problem is resolved in Release 12.1(27b)E. (CSCsa98860)
- A reload occurs when you delete a policy map that was attached in both the in and out direction. This problem is resolved in Release 12.1(27b)E. (CSCsb29774)
- When you configure an extended ACL that is using the same name as an active reflexive ACL a message appears, indicating that an error has occured in the system time and a traceback might occur. A software-forced reload also might occur when a standard ACL is configured using the same name as an active reflexive ACL. These problems occur when the reflexive timer expires. This problem is resolved in Release 12.1(27b)E. (CSCin85894)
- When you enter the IOS IP service level agreement (SLA) configuration command **rtr restart** to restart a probe, the probe is restarted and operates normally, but when you enter the **show rtr** configuration command, the following message is displayed:

  ```
  Status of Entry (SNMP RowStatus): notInService
  ```

  This problem is resolved in Release 12.1(27b)E. (CSCsa61284)
- When you enter the **show standby** command or the **show standby brief** command, a reload might occur. This problem occurs when multiple HSRP groups are configured or unconfigured while traffic for the HSRP groups is being processed. This problem is resolved in Release 12.1(27b)E. (CSCed83616)

FlexWAN Caveats

- Open FlexWAN Caveats in Release 12.1(27b)E2, page 129
- Resolved FlexWAN Caveats in Release 12.1(27b)E2, page 129
- Resolved FlexWAN Caveats in Release 12.1(27b)E1, page 129
- Resolved FlexWAN Caveats in Release 12.1(27b)E, page 129

Open FlexWAN Caveats in Release 12.1(27b)E2

None.

Resolved FlexWAN Caveats in Release 12.1(27b)E2

- When other modules have large configurations, an E1 controller on a PA-MC-8TE1+ port adapter might not be active following a reload. This problem is resolved in Release 12.1(27b)E2. (CSCin78110)
- With fair queuing configured on a T1 serial interface port adapter in a FlexWAN module, the **show interface** command might display a large number of output drops when there are no errors and no QoS drops. This problem is resolved in Release 12.1(27b)E2. (CSCsh31306)

Resolved FlexWAN Caveats in Release 12.1(27b)E1

- The SNMP IF MIB object ifInOctets might have a negative value for a multilink PPP interface. This problem occurs after all of these actions have occurred:
  - The multilink interface goes up and down several times.
  - The member links go up and down several times.
  - A CPE router connected to the multilink interface reloads.

  This problem is resolved in Release 12.1(27b)E1. (CSCsc33562)
- On an ATM PA-A3 port adapter, when a virtual circuit (VC) class that is configured for create on-demand is attached to the physical ATM interface and then the create on-demand configuration is removed and reapplied to the VC class, auto provisioning might get disabled. This problem is resolved in Release 12.1(27b)E1. (CSCin86455)
- An egress FlexWAN interface may go down when NBAR is configured on the ingress FlexWAN interface and when the egress FlexWAN interface has a thoughput of 2MBps or less throughput. This problem is resolved in Release 12.1(27b)E1. (CSCeh56032)

Resolved FlexWAN Caveats in Release 12.1(27b)E

- AppleTalk configured on a PA-A3 does not work for ATM VCs configured with AAL5NLPID encapsulations. This problem is resolved in Release 12.1(27b)E. (CSCeg67978)
- The controller on a PA-MC-STM1 port adapter does not come up after the system is reloaded. This problem is resolved in Release 12.1(27b)E. (CSCeg66282)
- All E1 interfaces on PA-MC-STM1 port adapters begin to go up and down, and then lose packets when they are pinging to remote POPs. This problem occurs on a FlexWAN module with at least 31 E1 interfaces configured and a small amount of FlexWAN RAM configured. This problem is resolved in Release 12.1(27b)E. (CSCef13901)

- When you use the **show controller** command to display the serial interface counters, they may stop incrementing for the input and output rate and the input and output packet counts. This problem occurs on a system configured with a PA-MC-E3 or a PA-MC-8E1 port adapter. The problem does not effect traffic flow. This problem is resolved in Release 12.1(27b)E. (CSCsa46643)
- A PA-MC-2T3+ port adapter configured in unchannelized mode might continuously generate the following traceback message while initializing:

  ```
  %SYS-2-INTSCHED: 'event dismiss' at level 2^M
  -Process= "Init", ipl= 2, pid= 3^M
  ```

  This problem is resolved in Release 12.1(27b)E. (CSCeh35783)
- A Multilink PPP (MLP) link does not forward traffic when MLP is configured on an interface of a FlexWAN port adapter, or an Enhanced FlexWAN PA. This problem is resolved in Release 12.1(27b)E. (CSCeb07656)
- An Any Transport over MPLS (AToM) virtual circuit that is configured on a PA-MC-8TE1+ stops forwarding traffic after the module is OIRd. This problem occurs when the PA-MC-8TE1+ is configured for Frame Relay over MPLS (FRoMPLS) or Ethernet interworking with Frame Relay and ATM. This problem is resolved in Release 12.1(27b)E. (CSCin67253)
- A channelized T3 interface might never come up after it is changed to unchannelized. This problem is resolved in Release 12.1(27b)E. (CSCin88048)

Service Module Caveats

- Open Service Module Caveats in Release 12.1(27b)E2, page 130
- Resolved Service Module Caveats in Release 12.1(27b)E2, page 130
- Resolved Service Module Caveats in Release 12.1(27b)E1, page 130
- Resolved Service Module Caveats in Release 12.1(27b)E, page 131

Open Service Module Caveats in Release 12.1(27b)E2

None.

Resolved Service Module Caveats in Release 12.1(27b)E2

None.

Resolved Service Module Caveats in Release 12.1(27b)E1

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml

  This problem is resolved in Release 12.1(27b)E1. (CSCsd75273)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml

  This problem is resolved in Release 12.1(27b)E1.(CSCse52951)

Resolved Service Module Caveats in Release 12.1(27b)E

None.

OSM Caveats

- Open OSM Caveats in Release 12.1(27b)E2, page 131
- Resolved OSM Caveats in Release 12.1(27b)E2, page 131
- Resolved OSM Caveats in Release 12.1(27b)E1, page 131
- Resolved OSM Caveats in Release 12.1(27b)E, page 131

Open OSM Caveats in Release 12.1(27b)E2

None.

Resolved OSM Caveats in Release 12.1(27b)E2

None.

Resolved OSM Caveats in Release 12.1(27b)E1

None.

Resolved OSM Caveats in Release 12.1(27b)E

- After frequent optical service module (OSM) online OIRs, you might see the following error message and a reload of the OSM.

  ```
  %FABRIC-SP-6-TIMEOUT_ERR: Fabric in slot 8 reported timeout error for channel 10
  (Module 4, fabric connection 0)
  ```

  This problem is resolved in Release 12.1(27b)E. (CSCef12193)
- On a Supervisor Engine 2, RSPAN does not work when configured on OSM Gigabit Ethernet LAN ports. This problem is resolved in Release 12.1(27b)E. (CSCsc24089)
- A system might learn MAC addresses from the wrong port. This problem occurs when the system is connected to an 802.1Q trunk with one of the subinterfaces configured for bridging. This problem only occurs for OSM-4GE-WAN-GBIC and OSM-2+4GE-WAN+ GE-WAN ports. This problem is resolved in Release 12.1(27b)E. (CSCed11719)
- A rounded shape and bandwidth parameter is not displayed when you enter the **show policy-map interface** *interface-name* command for an OSM module. This problem is resolved in Release 12.1(27b)E. (CSCsa80609)

Release 12.1(26)E and Rebuilds

- General Caveats, page 132
- FlexWAN Caveats, page 152
- Service Module Caveats, page 155
- OSM Caveats, page 157

Note The caveat lists for Release 12.1(26)E and rebuilds are updated frequently.

General Caveats

- Open General Caveats in Release 12.1(26)E9, page 132
- Resolved General Caveats in Release 12.1(26)E9, page 132
- Resolved General Caveats in Release 12.1(26)E8, page 134
- Resolved General Caveats in Release 12.1(26)E7, page 136
- Resolved General Caveats in Release 12.1(26)E6, page 139
- Resolved General Caveats in Release 12.1(26)E5, page 139
- Resolved General Caveats in Release 12.1(26)E4, page 141
- Resolved General Caveats in Release 12.1(26)E3, page 143
- Resolved General Caveats in Release 12.1(26)E2, page 143
- Resolved General Caveats in Release 12.1(26)E1, page 144
- Resolved General Caveats in Release 12.1(26)E, page 145

Open General Caveats in Release 12.1(26)E9

None.

Resolved General Caveats in Release 12.1(26)E9

- CSCin95836—Resolved in Release 12.1(26)E9.

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

- CSCse24889—Resolved in Release 12.1(26)E9.

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

  Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

  ```
  config t
  ip ssh version 1
  end
  ```

  Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

  10.1.1.0/24 is a trusted network that is permitted access to the router, all other access is denied

  ```
  access-list 99 permit 10.1.1.0 0.0.0.255
  access-list 99 deny any

  line vty 0 4
  access-class 99 in
  end
  ```

  Further Problem Description:

  For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tsec_c/part10/tsaclvty.htm

  For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

  http://www.cisco.com/warp/public/707/ssh.shtml

- CSCsg40567—Resolved in Release 12.1(26)E9.

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the ip http secure server command enabled.

  Workaround: Disable the **ip http secure server** command.

- CSCsg70474—Resolved in Release 12.1(26)E9.

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- Some UDP packets that have the Terminal Access Controller Access Control System (TACACS) port (49) as their destination might remain suspended in the interface queue. This problem occurs when TACACS+ is configured. This problem is resolved in Release 12.1(26)E9. (CSCsb11698)
- With RCP enabled, a reload might occur when the system receives a spoofed RCP packet that contains a specific data content. This problem is resolved in Release 12.1(26)E9. (CSCse05736)

Resolved General Caveats in Release 12.1(26)E8

- CSCse68138—Resolved in Release 12.1(26)E8.

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- A Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

  This problem is resolved in Release 12.1(26)E8. (CSCsb12598, CSCsb40304, CSCsd92405)

- Closing a Telnet session may cause a reload. This problem is resolved in Release 12.1(26)E8. (CSCds33629)
- In certain LAN topologies, the PIM assert mechanism can cause an upstream router to erroneously remove downstream interfaces from output interface lists. When this situation occurs, it causes multicast traffic to be dropped. This problem occurs when two or more upstream routers with routes to the same rendezvous point or traffic source are connected to the same LAN segment as two different downstream routers. The problem occurs when the two downstream routers select different upstream routers as their next hop. This problem is resolved in Release 12.1(26)E8. (CSCeh17756)
- A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

  This problem is resolved in Release 12.1(26)E8. (CSCsc64976)

- With the Cisco IOS Firewall CBAC feature enabled, if a client opens a connection to a server, which causes a firewall session to be created, and the connection is terminated on both the client and the server, the firewall session may never time out. This problem occurs with applications that use fixed source and destination ports. This problem is resolved in Release 12.1(26)E8. (CSCsc72722)
- Port 2 or port 4 on a WS-X6816-GBIC switching module might go up and down when port 1 is enabled, not connected, and set to autonegotiate. This problem occurs if a 1000BASE-T GBIC was ever inserted since the last time the module was reloaded. This problem is resolved in Release 12.1(26)E8. (CSCse12195)
- With a tunnel configured to use an ATM interface, one end of the tunnel cannot ping the other end until you bring either end of the tunnel interface down and up. This problem is resolved in Release 12.1(26)E8. (CSCse40423)
- A reload might occur when a routing event causes a Reverse Path Forwarding (RPF) interface to become an interface configured as a multicast boundary. This problem is resolved in Release 12.1(26)E8. (CSCse92050)
- A very slow memory leak might occur in the medium buffers. This problem occurs on a system configured with a distributed EtherChannel (DEC). When this problem occurs, MALLOCFAIL messages are displayed in the switch processor log. This problem is resolved in Release 12.1(26)E8. (CSCsf31542)
- The WS-X6516A-GBIC and the WS-X6548-GE-TX switching modules might fail the TestL3VlanMet, TestIngressSpan and TestEgressSpan diagnostic tests when they come online while the system is in flow-through mode. This problem is resolved in Release 12.1(26)E8. (CSCsg13124)
- When a PBR route map is currently using an ACL, and then you modify, configure, or reapply the ACL, TCAM entries might be programmed incorrectly and cause a connectivity problem. This problem occurs when the ACL is on a Supervisor Engine 2. This problem is resolved in Release 12.1(26)E8. (CSCse30376)

Resolved General Caveats in Release 12.1(26)E7

- The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

  This problem is resolved in Release 12.1(26)E7 (CSCek37177)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  This problem is resolved in Release 12.1(26)E7 (CSCek26492)

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

  This problem is resolved in Release 12.1(26)E7. (CCSCsd34759)

- Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

  Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

This problem is resolved in Release 12.1(26)E7. (CSCsd34855)

- Symptoms: Router may generate and/or forward crafted IP packets with the source IP address being the routers tunnel interface for GRE or mGRE tunnels. Incorrect packet decoding may be seen with "debug tunnel."

  Conditions: The router needs to receive a specially crafted GRE packet sent to the tunnel end-point. The outer IP packet must come from the configured tunnel source and be sent to the configured tunnel destination IP address Present Routed bit must be set to 1.

  Workaround: Upgrade Cisco IOS to a version containing fixes for: CSCuk27655 or CSCea22552 or CSCei62762.

  Further information: On the 6th September 2006, Phenoelit Group posted an advisory:

  Cisco Systems IOS GRE decapsulation fault

  Cisco's statement and further information are available on the Cisco public website at:

  http://www.cisco.com/warp/public/707/cisco-sr-20060906-gre.shtml

  This problem is resolved in Release 12.1(26)E7. (CSCei62762)

- A memory leak might occur when protocol filtering is enabled. This problem is resolved in Release 12.1(26)E7. (CSCsd45419)
- You might exceed the 255 buffer character limit for the **mac-address-table static** command if you enter too many interface names for the MAC in the same command. The following message is displayed:

  ```
  Enter configuration commands, one per line.  End with CNTL/Z.
  % Incomplete command.
  ```

  Workaround: Split the command that is specifying the interfaces into multiple commands. This problem is resolved in Release 12.1(26)E7. (CSCsc54552)
- SNMP version 3 user information might disappear after a switchover or a reload. This problem is resolved in Release 12.1(26)E7. (CSCsd22650)
- The multicast traffic rate might be displayed as low or zero when you enter the **show ip mroute active** command. This situation has no impact on performance because traffic is forwarded by hardware. This problem is resolved in Release 12.1(26)E7. (CSCsd51420)
- When you enter the **ip inspect** command for Structured Query Language (SQL) packets, a memory leak occurs in the IP input process. This problem is resolved in Release 12.1(26)E7. (CSCsb96107)
- Systems Network Architecture (SNA) packets are not bridged when VLAN 1025 is used on the bridged interface. When this problem occurs, SNA sessions cannot be established. This problem occurs on a Supervisor Engine 2. This problem is resolved in Release 12.1(26)E7. (CSCsc05015)
- Hardware switching is disabled because of an MLS CEF sanity failure after the following message is displayed:

  ```
  %MLSCEF-SP-2-FREEZE: hardware switching disabled on card
  ```

  This problem is resolved in Release 12.1(26)E7. (CSCsd64158)

- When polling the SNMP MIB object slbstickyobjectable, SNMP goes into a loop. No SNMP transactions take place and a loss of contact with SNMP devices may occur. This problem is resolved in Release 12.1(26)E7. (CSCeh54725)
- Intermediate System-to-Intermediate System (IS-IS) load balancing may not function correctly. This problem occurs in a topology in which three routers reside on a broadcast media. Router A is the root node that performs Shortest Path First (SPF) and has a direct path to both router B and router C. An additional path also also exists between router A and router B. When you configure IS-IS to enable router A to reach router C along two equal-cost paths, router A may continue to only use the additional path to router B to reach router C. This problem is resolved in Release 12.1(26)E7. (CSCea24421)
- Static routes that are redistributed into BGP display an incorrect next hop address. This situation might cause a routing loop. This problem is resolved in Release 12.1(26)E7. (CSCeg41727)
- With a Supervisor Engine 720, you might see software-forced reloads. This problem is resolved in Release 12.1(26)E7. (CSCed36177)

Resolved General Caveats in Release 12.1(26)E6

- When an MSFC2 creates a sticky ARP entry for a device in a private VLAN, the MSFC2 ages the ARP entry out when the ARP timer expires. This problem is resolved in Release 12.1(26)E6. (CSCej45800)
- A label might not be assigned for a peer provider edge (PE) device, which causes the label-controlled ATM (LC-ATM) label switch paths (LSPs) connectivity to be disrupted. This problem has a high impact on the operability of a virtual private network (VPN) configuration with multiple route reflectors (RRs) and label-controlled ATM (LC-ATM) links between PE routers. This problem is resolved in Release 12.1(26)E6. (CSCeb76341)

Resolved General Caveats in Release 12.1(26)E5

- Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

  Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

  This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

  Workaround: This advisory with appropriate workarounds is posted at

  http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

  This problem is resolved in Release 12.1(26)E5. (CSCeh73049)
- Occasionally, the PS-Fan status in the **show power** command displays n/a for a functional power supply. This problem is resolved in Release 12.1(26)E5. (CSCee01435)
- When the system uses an automatically learned source IP address to send packets, if the routes change and the new ACLs cannot forward the traffic, the IP address becomes stale and the transmission fails. If the system has not receive traffic from an IP address recently the outgoing interface is probably stale and it should be purged. This problem is resolved in Release 12.1(26)E5. (CSCei77073)

- SSH sessions might fail due to a bad packet length error when you open an SSH session from a Solaris or MacOSX client. The following message might appear:

  ```
  Disconnecting: Bad packet length -625118183.
  ```

  This problem is resolved in Release 12.1(26)E5. (CSCef33784)

- An autonomous system boundary router (ASBR) that is running open shortest path first (OSPF) and is configured with the **area** *area_id* **nssa default-information-originate** command, might continue to advertise a default route in a not-so-stubby area (NSSA) even after the default Border Gateway Protocol (BGP) route has been withdrawn and removed from the routing table. This problem is resolved in Release 12.1(26)E5. (CSCsc03828)

- Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors might reset unnecessarily on an interface that is configured with summarization. The summary on the interface regenerates when all components of the summary are lost and at least one component is relearned. When this problem occurs, the following message displayes:

  ```
  %DUAL-5-NBRCHANGE: IP-EIGRP 111: Neighbor x.x.x.x (FastEthernet4/0) is down: Summary
  up, remove external
  ```

  This problem is resolved in Release 12.1(26)E5. (CSCsc83334)

- While traffic is routed, a spurious access might occur if you repetitively reconfigure a service policy. This problem is resolved in Release 12.1(26)E5. (CSCej45192)

- Cisco Campus Manager user tracking might not display some neighbor hosts. This problem might occur when the router port has dynamically learned entries. This problem is resolved in Release 12.1(26)E5. (CSCsb97997)

- When the SNMP ifOperStatus MIB object for an interface that is a member of a multilink group is placed in the down state, the ifStackStatus entry that links the interface to the multilink group interface is removed from the IF-MIB. This problem is resolved in Release 12.1(26)E5. (CSCeh62084)

- The chassisFanStatus displays as a “minorFault” when you install a WS-C6509-NEB-A fan tray with one operational fan. This problem is resolved in Release 12.1(26)E5. (CSCsc28731)

- If you enter the **show power** command when a WS-F6K-PWR power module is installed in slot 8 or slot 9, the command displays “Unknown.” This problem does not affect operation. This problem is resolved in Release 12.1(26)E5. (CSCsb81734)

- Port-channel bundling fails during a switchover because of a difference in the trust values for the port channel and the members. The problem occurs when the following events occur in this order:
  - You have not enabled MLS QoS.
  - You created the port channel and applied the members.
  - You enabled MLS QoS.
  - You performed a switchover.

  This problem is resolved in Release 12.1(26)E5. (CSCdz90630)

- A Layer 3 VLAN interface might remain in the up/up state with no active corresponding Layer 2 interfaces. This problem occurs from the following sequence of events:
  - The Layer 3 VLAN interface is administratively shut down.
  - All of the corresponding Layer 2 ports become inactive, either because of disconnection or an administrative shut down.

  - While all corresponding Layer 2 ports remain inactive, the Layer 3 VLAN interface is administratively enabled (no shutdown).

  This problem is resolved in Release 12.1(26)E5. (CSCsc08947)

- The SNMP ifAdminStatus state for the ATM layer or the ATM Adaptation Layer 5 (AAL5) of an ATM interface or subinterface might go down. This situation can occur without entering a **shutdown** command, and prevents SNMP from monitoring the proper status of the ATM interfaces. This problem is resolved in Release 12.1(26)E5. (CSCsb12329)
- If traffic loss occurs when there is a high volume of broadcast traffic, the input broadcast counter increments and the input counter does not increment. Because the value of the SNMP ifHCInUCastPkts MIB object is the difference between the input counter and the input broadcast counter, the value of ifHCInUCastPkts might become negative. This problem is resolved in Release 12.1(26)E5. (CSCsc62574)
- The ports that are associated with a static MAC entry disappear from the **show mac-address-table** command static output, and the connectivity is disrupted. This problem occurs in either of the following ways:
  - With a static MAC address configured with the **disable-snooping** keyword, disable, and enable IGMP snooping.
  - With a static MAC address configured with the **disable-snooping** keyword and IGMP snooping enabled, delete, and reconfigure the static MAC address.

  This problem is resolved in Release 12.1(26)E5. (CSCsc36963)
- Packets that are going to be Layer 3 switched and are destined for a Hot Standby Router Protocol (HSRP) virtual MAC address (VMAC), are forwarded before the HSRP state becomes ACTIVE on the destination interface. This problem occurs when you enter the **shutdown** and **no shutdown** interface configuration commands on the destination interface. This problem is resolved in Release 12.1(26)E5. (CSCsb78050)

Resolved General Caveats in Release 12.1(26)E4

- A system configured with a summary address, which is also an OSPF not-so-stubby area (NSSA) area border router (ABR), might incorrectly age out and flush the summary address. This occurs when NSSA external type 1 or type 2 routes are present. This problem is resolved in Release 12.1(26)E4. (CSCsb28595)
- SLB real servers move to FAILED TESTING or READY_TO_TEST when a PROBE_ABDICATE event occurs. After this event occurs, the real servers will never become operational with per-packet virtual servers and Internet Control Message Protocol (ICMP) probes. This problem is resolved in Release 12.1(26)E4. (CSCsb14185)
- If an intermittent multicast source is inactive for 3.5 minutes, (S,G) entries in the MSDP cache might become inconsistent with a neighbor's cache which can cause multicast packet loss. This problem is resolved in Release 12.1(26)E4. (CSCsb23433)
- When a server farm is configured with two probes, and a real server is taken out of service and then brought back into service, one of the two probes configured for the server farm does not display the real server when you use the **show ip slb probe** command. This problem is resolved in Release 12.1(26)E4. (CSCsa73607)
- WCCP does not redirect traffic to cache engines from suppliers other than Cisco Systems if you do not configure a redirection port on the cache engine. This problem is resolved in Release 12.1(26)E4. (CSCei38603)
- The **snmp-server tftp-server-list** command fails to apply an access list for SNMP traffic. This problem is resolved in Release 12.1(26)E4. (CSCdu32036)

- You might see SCHED-3-THRASHING messages when an SSH client sends text at a high input rate. This problem is resolved in Release 12.1(26)E4. (CSCsa92622)
- A reload or spurious memory access occurs when HSRP rapidly changes states or goes up and down. This problem occurs with IOS SLB configured and with virtual servers that are monitoring these HSRP groups and probes that are configured on their server farms. This problem is resolved in Release 12.1(26)E4. (CSCin94752)
- The identification field in all TACACS+ packets is always 0 when the synchronize (SYN) flag is set and the TACACS+ packet goes through a filewall to the AAA server. The firewall interprets this 0 identification field as a Fragment Overlap Attack and drops additional new connections. This problem is resolved in Release 12.1(26)E4. (CSCeh48684)
- With both WCCP and NDE configured, you might see numerous tracebacks caused by alignment errors and CPU utilization might be unacceptably high. This problem is resolved in Release 12.1(26)E4. (CSCsb21972)
- With a Supervisor Engine 1, Cisco IOS firewall load-balancing connection objects are not built for non-TCP flows. This problem is resolved in Release 12.1(26)E4. (CSCsa88515)
- DLSw circuits are established over the same peer connection when DLSw load balancing is configured and when there are multiple peers that have the **dlsw icanreach mac-address** *mac_addr* command enabled with the same remote MAC address for the *mac_addr* argument. This problem is resolved in Release 12.1(26)E4. (CSCsa45750)
- If RIP on a CE router redistributes a default route into BGP on a PE router, and then that default route is redistributed back into RIP from a second CE router, the default route is not marked as poisoned or withdrawn on the first CE router when the link between the first CE router and the PE router is disconnected. This problem is resolved in Release 12.1(26)E4. (CSCeh06778)
- If two OSPF routing areas generate the same link-state advertisement (LSA) for a route and the route is known on the Area Border Router (ABR) as an intra-area route, a summary LSA might not be generated on the ABR if the route goes up and down. This problem is resolved in Release 12.1(26)E4. (CSCeg62496)
- With a Supervisor Engine 1, in rare circumstances, a reload might occur if you enter the **show mls ip** command. This problem is resolved in Release 12.1(26)E4. (CSCed00245)
- Erroneous “notPresent Temperature StatusValue Value =0” SNMP traps might be generated. This problem is resolved in Release 12.1(26)E4. (CSCsa91816)
- When a Web Cache Communication Protocol (WCCP) service is enabled, and mask assignment is configured as the assignment method, and five or more caches are in the service group, then protocol messages sent to the cache may overflow and cause memory corruption and a reload. This problem is resolved in Release 12.1(26)E4. (CSCeh56916)
- In rare situations a reload might occur, when there is a mix of Link State Advertisements (LSAs) that travel throughout the Autonomous System (Types 5 and 11) and LSAs that travel within a particular open shortest path first (OSPF) area (Types 1, 2, 3, 4, 6, 7, 9 and 10). This problem is resolved in Release 12.1(26)E4. (CSCef93215)
- Following a reload, an OSPF designated router (DR) might fail to regenerate the network link-state advertisement (LSA) when there is a shutdown interface with the same interface address in the OSPF area. This problem is resolved in Release 12.1(26)E4. (CSCee36721)
- If you configure aggressive OSPF hello timers and dead timers, then during periods of high CPU utilization, OSPF packets are not processed, and OSPF declares that OSPF neighbors are inoperative (“down”). This problem is resolved in Release 12.1(26)E4. (CSCec42160)

- In a multicast virtual private network (MVPN) environment with a provider edge (PE) router configuration and with the **ip pim register-rate-limit** global configuration command enabled, PIM register messages might not be sent for the default multicast distribution tree (MDT) to its rendezvous point (RP). This situation prevents PE routers from establishing PIM adjacencies with other PE routers in the MVPN. This problem is resolved in Release 12.1(26)E4. (CSCea59359)

Resolved General Caveats in Release 12.1(26)E3

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

  This problem is resolved in Release 12.1(26)E3. (CSCei61732)
- Receipt of a Border Gateway Protocol (BGP) Autonomous System (AS) path with a length that is equal to or greater than 255 might reset the BGP session. This problem is resolved in Release 12.1(26)E3. (CSCeh13489)

Resolved General Caveats in Release 12.1(26)E2

- If you are using the Open Shortest Path First (OSPF) protocol and the Catalyst 6500 series switch or the Cisco 7600 series router is an Area Border Router (ABR) attached to one or more not-so-stubby areas (NSSAs), the configuration of "summary-address 0.0.0.0 0.0.0.0" can result in the ABR default summary Link State Advertisement (LSA) being repeatedly flushed and reoriginated in each attached NSSA. This problem is resolved in Release 12.1(26)E2. (CSCdx83438)
- If a VPN routing/forwarding instance (VRF) static route points to a default route, an aggregate MultiProtocol Label Switching (MPLS) label is not applied. If this route address is redistributed, a VRF lookup is not performed and traffic is forwarded to the default interface and dropped. This problem is resolved in Release 12.1(26)E2. (CSCdy79465)
- When you use an **snmpget** command for an interface index below .1.3.6.1.2.1.31.1.1.1.6, the system responds with the following information:

  ```
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.12 : VARBIND EXCEPTION: No Such
  Instance.
  ```

  However, an **snmpwalk** executes successfully for an interface index below .1.3.6.1.2.1.31.1.1.1.6. This problem is resolved in Release 12.1(26)E2.(CSCef79968)
- After multiple RPR+ switchovers, additional SNMP version 3 configurations might be added to the configuration file. This problem is resolved in Release 12.1(26)E2. (CSCeg00304)
- If you insert a CSM in a running system, and then reset the module by entering the **hw-module module** *module slot number* **reset** command, the active supervisor engine resets. This problem is resolved in Release 12.1(26)E2. (CSCeg77264)
- A routing table entry for a Cisco IOS Server Load Balancing (SLB) virtual server is removed when the IP address of the virtual server is advertised as active for the host route and the backup server farm takes over. As a result, connectivity is lost to the backup server farm virtual server and its real servers. This problem is resolved in Release 12.1(26)E2.(CSCeh17417)

- When EoMPLS is configured on a system that is functioning as the PE router and a FlexWAN module is used to connect to the core router, packets sent by the CE router are dropped. This problem is resolved in Release 12.1(26)E2. (CSCei01835)
- The system may reset if it receives a invalid VTP packet. The invalid VTP packet must be received on a port configured for ISL or 802.1q trunking and must correctly match the VTP domain name. This problem does not affect switch ports configured for the voice VLAN. This problem is resolved in Release 12.1(26)E2. (CSCsa67294)
- A system with a Supervisor Engine 2 and an MSFC2 may experience a memory leak in a CEF IPC background process on the route processor and on the switch processor during stress testing that introduces routing instability. This problem is resolved in Release 12.1(26)E2. (CSCsa83923)
- When a port is configured as a SPAN destination port, multicast traffic that is generated or processed by the system floods the SPAN destination port and overruns any legitimate SPAN packets. This problem is resolved in Release 12.1(26)E2. (CSCsa87021)

Resolved General Caveats in Release 12.1(26)E1

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in Release 12.1(26)E1. (CSCef60659, CSCsa59600, CSCef44699)
- If you configure fallback bridging on a Layer 3 LAN port, established OSPF neighbors might be put into the INIT state. This problem is resolved in Release 12.1(26)E1. (CSCef66899)
- With a Supervisor Engine 2, QoS does not preserve the CoS value derived from IP precedence in traffic that originates on the MSFC2. This problem is resolved in Release 12.1(26)E1. (CSCef68801)

- With Per-VLAN-Spanning Tree (PVST) configured, if you remove a DFC-equipped switching module, other DFC-equipped switching modules might retain some Layer 2 address entries for the removed module. Traffic loss occurs when the remaining DFC-equipped switching modules send traffic to the removed module. This problem is resolved in Release 12.1(26)E1. (CSCef84129)
- Layer 2 EtherChannels configured with ports on different DFC-equipped switching modules periodically purge and refresh their Layer 2 address tables. Typically, the refresh takes a few seconds as the EtherChannel learns the destination MAC addresses, during which time the EtherChannel floods all egress traffic to other ports in the VLAN as unknown unicast traffic. With a Layer 2 EtherChannel configured with ports on different DFC-equipped switching modules, the EtherChannel might flood traffic for several minutes. This problem is resolved in Release 12.1(26)E1. (CSCeg39091)
- With a Supervisor Engine 2, a memory leak might occur in the medium buffers. This problem is resolved in Release 12.1(26)E1. (CSCsa47573)
- If you enter the logging event link-status interface command for a Layer 2 port-channel interface and save the configuration, the command is not present in the configuration file following bootup or a reload. This problem is resolved in Release 12.1(26)E1. (CSCsa48616)

Resolved General Caveats in Release 12.1(26)E

- In VTP transparent mode, the VLAN database might be lost after a VTP configuration error occurs. This problem is resolved in Release 12.1(26)E. (CSCef47414)
- When an EXEC session is at the “More” prompt, the session fails to time out. This problem is resolved in Release 12.1(26)E. (CSCef35192)
- SNMP traps are sent for every Internet Key Exchange (IKE) timeout and rekey but not for every IPsec timeout and rekey. This situation might generate many false alerts that an IKE tunnel is down when the IKE tunnel is torn down but immediately rebuilt. Releases where CSCee91044 is resolved do not send SNMP traps that are sent for normal IKE operation. This problem is resolved in Release 12.1(26)E. (CSCee91044)
- Several MIB entity tables share one entCacheFlag and under rare circumstances, accessing the MIB entity tables might cause an entCacheFlag state that is not valid for all the MIB entity tables and a reload might occur. This problem is resolved in Release 12.1(26)E. (CSCeg19038)
- With OSPF routing configured, and with default routes learned from multiple autonomous system boundary routers (ASBRs) as equal cost paths, reconfiguring the cost of one of the interfaces for the default routes does not correctly update the routing table. This problem is resolved in Release 12.1(26)E. (CSCee16068)
- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command ‘bgp log-neighbor-changes’ configured are vulnerable. The BGP protocol is not

enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

This problem is resolved in Release 12.1(26)E. (CSCee67450)

- A VACL configured on a VLAN drops non-IP packets if there is no Layer 3 VLAN interface configured for that VLAN. This problem is resolved in Release 12.1(26)E. (CSCef09904)
- The **interface range** command syntax requires spaces. This problem is resolved in Release 12.1(26)E. (CSCin82081)
- With NAT configured, if you enter an **ip multicast boundary** command that uses an ACL that denies multicast traffic, and if you then reconfigure the ACL to permit the multicast traffic, the multicast traffic continues to be denied. This problem is resolved in Release 12.1(26)E. (CSCin84133)
- You can enter a **no service-policy input** command without entering the service policy name. This problem is resolved in Release 12.1(26)E. (CSCin83726, CSCin83727)
- The TACACS+ log displays "group-async" instead of "gigabitethernet" for Gigabit Ethernet ports. This problem is resolved in Release 12.1(26)E. (CSCef94543)
- After a reload, multicast sources in secondary IP subnets cannot register immediately. This problem is resolved in Release 12.1(26)E. (CSCsa39767)
- A reload might occur if you enable and disable port security repeatedly on a range of ports. This problem is resolved in Release 12.1(26)E. (CSCin84166)
- After a switchover to a redundant supervisor engine, aggregate policers might not be applied to the interfaces where they are configured. This problem is resolved in Release 12.1(26)E. (CSCin83227)
- An ACL with no ACEs does not deny traffic when it is applied to an unstable port-channel interface that is part of a multicast stub network. This problem is resolved in Release 12.1(26)E. (CSCin82441)
- When you reconfigure the forwarding method for a cache engine service from Layer 2 redirection to GRE tunneling, the MLS flow mask is not amended appropriately. This situation might cause suboptimal performance. This problem is resolved in Release 12.1(26)E. (CSCin79644)
- The default severity level is 6 instead of 3 for many system messages from these modules:
  - Supervisor Engine 1
  - Supervisor Engine 2
  - WS-X6408-GBIC
  - WS-X6408A-GBIC
  - WS-X6416-GE-MT
  - WS-X6416-GBIC
  - WS-X6516-GBIC
  - WS-X6516A-GBIC

  - WS-X6816-GBIC
  - WS-X6316-GE-TX
  - WS-X6516-GE-TX

  This problem is resolved in Release 12.1(26)E. (CSCeg12816)

- The hardware switching information for (*,G) multicast traffic might not be consistent with the software routing table. This problem is resolved in Release 12.1(26)E. (CSCeg13661)
- A memory leak occurs when IGMP snooping is configured. This problem is resolved in Release 12.1(26)E. (CSCeg13033)
- The BPDU guard feature does not work on an access port when you configure a voice VLAN unless either the voice VLAN or the access VLAN is VLAN 1. This problem is resolved in Release 12.1(26)E. (CSCef93371)
- The SNMP portEntPhysicalIndex MIB object is not implemented for the WS-X6316-GE-TX switching module. This problem is resolved in Release 12.1(26)E. (CSCef83162)
- With multicast support configured, the order-dependent ACL merge (ODM) algorithm fails when you configure context-based access control (CBAC). This problem is resolved in Release 12.1(26)E. (CSCef80725)
- IEEE 802.1X port-based authentication might not work if it is enabled on more than 50 ports. This problem is resolved in Release 12.1(26)E. (CSCef75501)
- With policy-based routing (PBR) configured, you might see “ALIGN-3-SPURIOUS” and “ALIGN-3-TRACE” messages. This problem is resolved in Release 12.1(26)E. (CSCef70083)
- Among BGP peers, the withdraw update message might be couurpt for the multicast BGP address family (AF). This problem is resolved in Release 12.1(26)E. (CSCef68244)
- With power supplies of significantly different wattages in an OSR-7609 or WS-C6509-NEB chassis, a reload might occur when a module powers up. This problem is resolved in Release 12.1(26)E. (CSCef62539)
- When the BGP table is full on an MPLS backbone router, routing updates or configuring additional routes might cause a reload. This problem is resolved in Release 12.1(26)E. (CSCef49199)
- When the routers in the core of an MPLS VPN environment are configured as iBGP peers, routes learned by provider edge (PE) routers are not propagated through iBGP to other PE routers. This problem is resolved in Release 12.1(26)E. (CSCef44819)
- Following a reload when multicast routing and PIM are configured, the **no mls ip multicast non-rpf cef** command appears in the configuration file. This problem is resolved in Release 12.1(26)E. (CSCef36986)
- If you configure a SPAN destination port on any of these modules, and the SPAN destination port goes down and comes back up, ingress traffic through other ports on the same port ASIC as the SPAN destination port might experience high latency:
  - Supervisor Engine 1
  - Supervisor Engine 2
  - WS-X6408-GBIC
  - WS-X6408A-GBIC
  - WS-X6416-GE-MT
  - WS-X6416-GBIC
  - WS-X6516-GBIC

  - WS-X6516A-GBIC
  - WS-X6816-GBIC
  - WS-X6316-GE-TX
  - WS-X6516-GE-TX

  This problem is resolved in Release 12.1(26)E. (CSCef32513)

- When configured as an IEEE 802.1Q trunk, ports on these modules might drop all native VLAN traffic:
  - Supervisor Engine 1
  - Supervisor Engine 2
  - WS-X6408-GBIC
  - WS-X6408A-GBIC
  - WS-X6416-GE-MT
  - WS-X6416-GBIC
  - WS-X6516-GBIC
  - WS-X6516A-GBIC
  - WS-X6816-GBIC
  - WS-X6316-GE-TX
  - WS-X6516-GE-TX

  This problem is resolved in Release 12.1(26)E. (CSCef23302)

- With Cisco IOS SLB configured, administrative connections might be unresponsive with messages similar to these being displayed:

```
%ICC-5-WATERMARK: 938 pkts for class SLB_PURGE_REQUESTS are waiting to be processed
%IPC-5-WATERMARK: 941 messages pending in xmt for the port (10000.5) seat 10000
```

  This problem is resolved in Release 12.1(26)E. (CSCef13273)

- Multicast BGP routes that are being advertised by an upstream BGP neighbor might be deleted from the multicast BGP routing table. This problem is resolved in Release 12.1(26)E. (CSCef08822)
- When you configure a static PIM rendezvous point (RP) IP address with an ACL that specifies the groups for the RP, and there is also another RP IP address configured without an ACL, you cannot remove the first RP IP address from the configuration. This problem is resolved in Release 12.1(26)E. (CSCee93574)
- A reload might occur if you enter the **show ip msdp peer** command when any multicast source discovery protocol (MSDP) sessions are unstable. This problem is resolved in Release 12.1(26)E. (CSCee88542)
- The maximum value displayed for VRF multicast route uptime is seven weeks. This problem is resolved in Release 12.1(26)E. (CSCee84457)
- The **show** commands that display files stored on flash devices might not display the file type correctly. This problem is resolved in Release 12.1(26)E. (CSCee80595)
- With RPR+ redundancy configured, Cisco IOS reflexive ACLs might not work after switchover to the redundant supervisor engine. This problem is resolved in Release 12.1(26)E. (CSCee79876)
- Policing might not be accurate for packets smaller than 82 bytes. This problem is resolved in Release 12.1(26)E. (CSCee78451)

- A reload might occur when a distance vector multicast routing protocol (DVMRP) tunnel is configured and routing information is being redistributed between DVMRP and MBGP. This problem is resolved in Release 12.1(26)E. (CSCee66936)
- With policy-based routing (PBR) and an input ACL configured on the same interface, if you enter the **clear arp-cache** command, PBR is done in software instead of hardware. This problem is resolved in Release 12.1(26)E.(CSCee58127)
- If you enter the **attach** command through the Cisco IOS web browser interface, a reload might occur. This problem is resolved in Release 12.1(26)E. (CSCee56618)
- If you enter the **debug ip slb connections acl** command, the debugging output might consume all available resources. This problem is resolved in Release 12.1(26)E with the **debug ip slb connections** [**state**] [*acl_name*] command. (CSCee33923)
- With a PFC2 or DFCs, you might see "L3-PS-DRVR" messages. This problem is resolved in Release 12.1(26)E. (CSCee24424)
- With Cisco IOS SLB configured, a reload might occur if you remove the SLB configuration while the SLB virtual servers are handling traffic. This problem is resolved in Release 12.1(26)E. (CSCee23087)
- When an OSPF neighbor on a local IP segment has multiple interfaces on that IP segment, OSPF installs only a single next-hop entry to routes reachable through the OSPF neighbor, instead of multiple next-hop entries, as required by RFC 2328. This problem is resolved in Release 12.1(26)E. (CSCee21928)
- With Cisco IOS SLB configured, you might see "ALIGN-3-SPURIOUS" messages. This problem is resolved in Release 12.1(26)E. (CSCed58748)
- After a reload, the bridge ID MAC address of a bridge group might change. This problem is resolved in Release 12.1(26)E. (CSCed38840)
- If you enable PIM on a VLAN interface and configure a bridge group on the VLAN interface, and then remove the PIM configuration from the VLAN interface, EIGRP neighborships are lost. This problem is resolved in Release 12.1(26)E. (CSCed12722)
- With a Y-cable Automatic Protection Switching (APS) configuration, there might be 30 to 45 seconds of traffic loss following an APS switchover. This problem is resolved in Release 12.1(26)E. (CSCdz66609)
- The "Do Not Learn" bit is not set in Layer 2 traffic processed by bridge groups on the MSFC. This problem is resolved in Release 12.1(26)E. (CSCeb56814)
- If you change the configuration of a permanent virtual circuit (PVC) after an alarm indication signal (AIS) is received on the PVC, the PVC does not come up; additionally, the PVC does not come up after the AIS stops. This problem is resolved in Release 12.1(26)E. (CSCdy04914)
- When configured as a provider edge (PE) router, IP path MTU discovery does not work from directly connected network devices. For example, IP path MTU discovery might not work between BGP peers. This problem is resolved in Release 12.1(26)E. (CSCds90697)
- Configuring an extended Border Gateway Protocol (BGP) community-list statement with any illegal regular expression pattern might cause a reload. This problem is resolved in Release 12.1(26)E. (CSCdx71842)
- After you enter a **shutdown** command on a physical ATM interface, ATM subinterfaces configured on the physical ATM interface are displayed as "down" instead of "administratively down." This problem is resolved in Release 12.1(26)E. (CSCea92873)
- The allowed VLAN list does not filter the traffic transmitted from a SPAN destination trunk port. This problem is resolved in Release 12.1(26)E. (CSCeb01318)

- For QoS filtering, extended ACLs that are configured to match DSCP parse 7 bits of the ToS byte instead of 6 bits. This problem is resolved in Release 12.1(26)E. (CSCec86976)
- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in Release 12.1(26)E. (CSCed78149, CSCef44225)
- In IP packets with the IP options field populated, the IP type-of-service (ToS) byte might be truncated to a 3-bit long field. This problem deletes 3 bits of the 6-bit DSCP value and causes incorrect QoS operation. This problem is resolved in Release 12.1(26)E. (CSCed93264)
- With a default route configured, a reload might occur if you enter the **clear ip route *** command. This problem is resolved in Release 12.1(26)E. (CSCee35125)
- A reload might follow the display of these messages:

```
%RPC-SP-2-FAILED: Failed to send RPC request online_diag_sp_request:get_rp_cpu_info
-Traceback= 40929C90 4067A8F0 40683EB8 406609D4 406612C0 40661DAC 40660040 4065FEB8
%Software-forced reload
Unexpected exception, CPU signal 23, PC = 0x4013E95C
-Traceback= 4013E95C 4013C824 40929C98 4067A8F0 40683EB8 406609D4 406612C0 40661DAC
40660040 4065FEB8
```

  This problem is resolved in Release 12.1(26)E. (CSCee36959)
- Traffic is routed in software when it uses a static ARP entry with an IP route that has a destination that is a local interface instead of an IP next-hop address. A static ARP entry created after a dynamic ARP has been learned prevents the updating of the dynamic ARP entry. This problem is resolved in Release 12.1(26)E. (CSCee49121)
- In an MPLS VPN provider edge (PE) configuration, for prefixes with multiple paths, some of which are on an OIRed switching module, the local label for a prefix in the label forwarding information base (LFIB) might be different from the local label allocated by the Label Distribution Protocol

(LDP). To display the LFIB local label, enter the **show mpls forwarding prefix** command. To display the LDP-allocated local label, enter the **show mpls ldp binding prefix mask length** command. This problem is resolved in Release 12.1(26)E. (CSCee72857)

- In switch-fabric "bus" mode with either WS-X6516A-GBIC or WS-X6548-GE-TX switching modules installed, some ingress SPAN traffic is duplicated. This problem is resolved in Release 12.1(26)E. (CSCee78323)
- With multicast support configured on a Supervisor Engine 2, VACLs do not capture traffic for RSPAN. This problem is resolved in Release 12.1(26)E. (CSCef07017)
- A memory leak might occur with Cisco IOS firewall authentication proxy configured. This problem is resolved in Release 12.1(26)E. (CSCef14971)
- After you enter the **squeeze** command for a 32-MB bootflash device, you cannot write any files to the bootflash. This problem is resolved in Release 12.1(26)E. (CSCef15418)
- With a Supervisor Engine 1, copying files with TFTP takes longer than usual because many corrected errors occur during the copy process. This problem is resolved in Release 12.1(26)E. (CSCef26370)
- With a Supervisor Engine 2, the software and hardware CEF tables might not be consistent with each other. This problem is resolved in Release 12.1(26)E. (CSCef27359)
- Using SNMP to change the name of VLAN 1002, 1003, 1004, or 1005 causes a traceback and corrupts the VLAN database. This problem is resolved in Release 12.1(26)E. (CSCef43000)
- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

  The Advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

  This problem is resolved in Release 12.1(26)E. (CSCef46191)
- In rare situations, a reload might occur if you enter the **show mls qos ip** command. This problem is resolved in Release 12.1(26)E. (CSCef50318)
- A VACL can match BPDUs. Spanning tree loops can occur if the VACL drops or redirects the BPDUs. This problem is resolved in Release 12.1(26)E. (CSCef58932)
- Over an SSHv2 connection, the output from a command that displays many lines of text pauses until you press a key. This problem is resolved in Release 12.1(26)E. (CSCef61978)
- With a Supervisor Engine 1 and an MSFC2, when the TCAM mask utilization reaches approximately 50 percent, you might see these TCAM mask exception messages:

```
00:11:17: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
00:11:17: %QM-SP-4-WARNING: TCAM request replace [lkup=2] status:1
00:11:17: SP: TCAM ASSERT FAILURE: label_alloc_tbl[label].num_if_using[lookup_type]
!= 0: ../const/native-sp/tcam_label.c: 1379
00:11:17: SP: -Traceback= 603C1090 603ACAE0 603AA018 603B7F38 603B8994 6039CE5C
603A53B8 6039D110 6039D254 6039D360 6039D6B4 6039D8E0 600FA6CC 600FA6B8
```

  This problem is resolved in Release 12.1(26)E. (CSCef73019)

- Some IP traffic might be sent with incorrect alignment, and you might see "ALIGN-SP-3-CORRECT: Alignment correction made" messages. This problem is resolved in Release 12.1(26)E. (CSCef73076)
- In rare situations, the MSFC might stop responding to received traffic. This problem is resolved in Release 12.1(26)E. (CSCef85654)
- When the number of routing table entries exceeds the capacity of the hardware-forwarding information base (FIB), the routing table entry for a default route might change so that traffic is dropped instead of forwarded. This problem is resolved in Release 12.1(26)E. (CSCin78197)
- After a reload, or following a switchover to a redundant supervisor engine, service policies that were attached to Layer 3 VLAN interfaces are missing. This problem is resolved in Release 12.1(26)E. (CSCin80578)
- A reload might occur if the order-dependent ACL merge (ODM) algorithm fails. This problem is resolved in Release 12.1(26)E. (CSCin83455)
- IEEE 802.1X port-based authentication might not work if it is enabled on more than 50 ports. This problem is resolved in Release 12.1(26)E. (CSCin83972)

FlexWAN Caveats

- Open FlexWAN Caveats in Release 12.1(26)E9, page 152
- Resolved FlexWAN Caveats in Release 12.1(26)E9, page 152
- Resolved FlexWAN Caveats in Release 12.1(26)E8, page 152
- Resolved FlexWAN Caveats in Release 12.1(26)E7, page 153
- Resolved FlexWAN Caveats in Release 12.1(26)E6, page 153
- Resolved FlexWAN Caveats in Release 12.1(26)E5, page 153
- Resolved FlexWAN Caveats in Release 12.1(26)E4, page 153
- Resolved FlexWAN Caveats in Release 12.1(26)E3, page 153
- Resolved FlexWAN Caveats in Release 12.1(26)E2, page 153
- Resolved FlexWAN Caveats in Release 12.1(26)E1, page 153
- Resolved FlexWAN Caveats in Release 12.1(26)E, page 154

Open FlexWAN Caveats in Release 12.1(26)E9

None.

Resolved FlexWAN Caveats in Release 12.1(26)E9

None.

Resolved FlexWAN Caveats in Release 12.1(26)E8

- On an ATM PA-A3 port adapter, when a virtual circuit (VC) class that is configured for create on-demand is attached to the physical ATM interface and then the create on-demand configuration is removed and reapplied to the VC class, auto provisioning might get disabled. This problem is resolved in Release 12.1(26)E8. (CSCin86455)

Resolved FlexWAN Caveats in Release 12.1(26)E7

- A reload caused by a bus error might occur on a FlexWAN module configured with serial port adapters after this error message is displayed:

  ```
  FIB-3-FIBDISABLE: Fatal error, slot/cpu 4/0: Linecard timed out waiting for messages
  from RP.
  ```

  This problem occurs after the serial interfaces that are part of a multilink interface go up and down. This problem is resolved in Release 12.1(26)E7. (CSCsc44130)
- A POS interface on a FlexWAN module might be suspended in the up or down state after an upgrade to Release 12.1(26)E6. This problem is resolved in Release 12.1(26)E7. (CSCsd40136)

Resolved FlexWAN Caveats in Release 12.1(26)E6

None.

Resolved FlexWAN Caveats in Release 12.1(26)E5

- If you perform an OIR on a PA-MC-STM-1 port adapter that is configured to support automatic protection switching (APS), a CBUS-3-CCBCMDFAIL1 message might display. This problem is resolved in Release 12.1(26)E5. (CSCeg06570)
- With a FlexWAN module, when you enter the **fair-queue aggregate-limit** command or the **fair-queue individual-limit** command, the currently running configurations do not change and the sizes of the queues do not change to the configured values. This problem is resolved in Release 12.1(26)E5. (CSCsa98325)

Resolved FlexWAN Caveats in Release 12.1(26)E4

- With Cisco IOS SLB configured, FlexWAN module ingress traffic is hardware switched instead of route-cache switched after a switchover. This problem is resolved in Release 12.1(26)E4. (CSCsa43553)
- FlexWAN module POS interfaces stay down after a reload. This problem is resolved in Release 12.1(26)E4. (CSCei68284)

Resolved FlexWAN Caveats in Release 12.1(26)E3

None.

Resolved FlexWAN Caveats in Release 12.1(26)E2

None.

Resolved FlexWAN Caveats in Release 12.1(26)E1

None.

Resolved FlexWAN Caveats in Release 12.1(26)E

- When you modify the configuration of a serial interface, you might see messages similar to these:

  ```
  %INTERFACE_API-3-NODESTROYSUBBLOCK: The HWIDB subblock named COPS_PR was not removed
  -Traceback=
  ```

  This problem is resolved in Release 12.1(26)E. (CSCin65698)
- The output packet counter for multilink and distributed link fragmentation and interleaving (dLFI) interfaces displays double the actual traffic count. This problem is resolved in Release 12.1(26)E. (CSCin40374)
- Variable bit rate (VBR) permanent virtual circuits (PVCs) on ATM OC3 port adapters might not pass any traffic. This problem is resolved in Release 12.1(26)E. (CSCeg29906)
- With a Supervisor Engine 2 and a PA-MC-8TE1+ port adapter, the E1 interfaces might stay down after switchover to a redundant supervisor engine. This problem is resolved in Release 12.1(26)E. (CSCeg11283)
- The SNMP ifAdminStatus MIB object does not support ATM subinterfaces. This problem is resolved in Release 12.1(26)E. (CSCeg03153)
- With more than 38 multilink bundles configured on a port adapter, a reload might occur if CEF switching is disabled. This problem is resolved in Release 12.1(26)E. (CSCef94525)
- With an E3 serial port adapter, when you enter the **dsu bandwidth** *kbps_rate* command, the DSU bandwidth might not change. This problem is resolved in Release 12.1(26)E. (CSCef73120)
- On a PA-MC-2T3+ port adapter, serial subrate interfaces do not follow the up or down state of the port adapter controller. This problem is resolved in Release 12.1(26)E. (CSCef61641)
- With a PA-MC-STM1 port adapter, in some topologies the **clock source line** command does not work and is not saved in the configuration. This problem is resolved in Release 12.1(26)E. (CSCef56327)
- With non-real time variable bit rate (VBR-nrt) shaping configured on more than one permanent virtual circuit (PVC) defined under the same physical ATM interface on a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter, when the load is equal to or greater than the maximum configured VBR-nrt value on at least two PVCs, not all of the PVCs achieve the configured VBR-nrt value. This problem is resolved in Release 12.1(26)E. (CSCef55463)
- When a PA-MC-2T3+ goes down for a short time and an alarm occurs, the port adapter does not report the type of alarm. This problem is resolved in Release 12.1(26)E. (CSCee49983)
- Following a reload, the **vbr-nrt** command might be missing from inverse multiplexing over ATM (IMA) interfaces. This problem is resolved in Release 12.1(26)E. (CSCec51408)
- High traffic flow rates (for example, 60 percent or more of capacity) through a PA-A3 ATM port adapter might cause a reload. This problem is resolved in Release 12.1(26)E. (CSCdy46272)
- The PA-MC-2T3+ port adapter does not delay for two seconds before bringing down the T3 controller in the event of an alarm as required by the ANSI T1.231 specification. This problem is resolved in Release 12.1(26)E. (CSCee49862)
- The PA-2T3+ port adapter does not delay for two seconds before bringing down the T3 controller in the event of an alarm as required by the ANSI T1.231 specification. This problem is resolved in Release 12.1(26)E. (CSCee70591)
- 1,500-byte pings fail on a PA-A3 ATM subinterface configured for MPLS and configured with the **ip mtu 1500** command. This problem is resolved in Release 12.1(26)E. (CSCef91994)

- Under a high traffic load, a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter might display an increasing “rx_no_buffer” counter in the output of the **show controllers atm** privileged EXEC command, and some PVCs that are configured on the port adapter might stop receiving traffic. This problem is resolved in Release 12.1(26)E. (CSCin77553)
- Serial interfaces on a PA-MC-8TE1+ port adapter that are configured as part of a channel group continue to process packets when the interface is in the “admindown” state. The counters in the output of the **show interfaces serial** command might increment when the serial interface is shut down. This problem is resolved in Release 12.1(26)E. (CSCin78325)

Service Module Caveats

- Open Service Module Caveats in Release 12.1(26)E9, page 155
- Resolved Service Module Caveats in Release 12.1(26)E9, page 155
- Resolved Service Module Caveats in Release 12.1(26)E8, page 155
- Resolved Service Module Caveats in Release 12.1(26)E7, page 156
- Resolved Service Module Caveats in Release 12.1(26)E6, page 156
- Resolved Service Module Caveats in Release 12.1(26)E5, page 156
- Resolved Service Module Caveats in Release 12.1(26)E4, page 156
- Resolved Service Module Caveats in Release 12.1(26)E3, page 156
- Resolved Service Module Caveats in Release 12.1(26)E2, page 156
- Resolved Service Module Caveats in Release 12.1(26)E1, page 156
- Resolved Service Module Caveats in Release 12.1(26)E, page 156

Open Service Module Caveats in Release 12.1(26)E9

None.

Resolved Service Module Caveats in Release 12.1(26)E9

None.

Resolved Service Module Caveats in Release 12.1(26)E8

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml

  This problem is resolved in Release 12.1(26)E8. (CSCsd75273)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml

  This problem is resolved in Release 12.1(26)E8. (CSCse52951)
- You might not be able to ping a Fast Ethernet interface or a Gigabit Ethernet interface that is on a communication media module (CMM) from the same subnet. This problem is resolved in Release 12.1(26)E8. (CSCsf29400)
- A Cisco Discovery Protocol (CDP) duplex mismatch might occur in which a Fast Ethernet interface on the supervisor engine is in half-duplex mode and the corresponding Fast Ethernet interface on a communication media module (CMM) is in full-duplex mode. This problem is resolved in Release 12.1(26)E8. (CSCse98596)

Resolved Service Module Caveats in Release 12.1(26)E7

None.

Resolved Service Module Caveats in Release 12.1(26)E6

None.

Resolved Service Module Caveats in Release 12.1(26)E5

None.

Resolved Service Module Caveats in Release 12.1(26)E4

- Do not enable Cisco Discovery Protocol (CDP) on Firewall Services Module (FWSM) gigabyte interfaces *slot_number*/2 through *slot_number*/6. This problem is resolved in Release 12.1(26)E4. (CSCsa74926)

Resolved Service Module Caveats in Release 12.1(26)E3

None.

Resolved Service Module Caveats in Release 12.1(26)E2

None.

Resolved Service Module Caveats in Release 12.1(26)E1

None.

Resolved Service Module Caveats in Release 12.1(26)E

- The trunk connection to a WS-X6066-SLB-APC Content Switching Module (CSM) carries VLANs that are not used by the CSM. This problem is resolved in Release 12.1(26)E. (CSCeg41623)

OSM Caveats

- Open OSM Caveats in Release 12.1(26)E9, page 157
- Resolved OSM Caveats in Release 12.1(26)E9, page 157
- Resolved OSM Caveats in Release 12.1(26)E8, page 157
- Resolved OSM Caveats in Release 12.1(26)E7, page 157
- Resolved OSM Caveats in Release 12.1(26)E6, page 157
- Resolved OSM Caveats in Release 12.1(26)E5, page 157
- Resolved OSM Caveats in Release 12.1(26)E4, page 157
- Resolved OSM Caveats in Release 12.1(26)E3, page 158
- Resolved OSM Caveats in Release 12.1(26)E2, page 158
- Resolved OSM Caveats in Release 12.1(26)E1, page 158
- Resolved OSM Caveats in Release 12.1(26)E, page 158

Open OSM Caveats in Release 12.1(26)E9

None.

Resolved OSM Caveats in Release 12.1(26)E9

None.

Resolved OSM Caveats in Release 12.1(26)E8

- Traffic passing on an interface from a traffic generator to the second port on a OSM-2+4GE-WAN+ module might lose approximately one packets every minute. This problem occurs when the traffic generator is configured to generate IPv4 TCP/UDP packets with a data pattern of Random only. This problem is resolved in Release 12.1(26)E8. (CSCsd88401)

Resolved OSM Caveats in Release 12.1(26)E7

- Egress packets might be dropped or delayed on an Optical Services Module (OSM). This problem occurs when Hierarchical Modular QoS CLI (MQC) is applied to the subinterfaces. This problem is resolved in Release 12.1(26)E7. (CSCsd40172)

Resolved OSM Caveats in Release 12.1(26)E6

None.

Resolved OSM Caveats in Release 12.1(26)E5

None.

Resolved OSM Caveats in Release 12.1(26)E4

- Disposition packets that are index-directed from a core-facing OSM are not passed to a CE-facing channelized OSM. This problem is resolved in Release 12.1(26)E4. (CSCeh29617)

- With Quality of Service (QoS) configured on multiple OSM subinterfaces, the OSM might reload after a Route Processor Redundancy Plus (RPR+) switchover. This problem is resolved in Release 12.1(26)E4. (CSCsa77560)
- With MPLS support configured, a reload might occur when you configure an ATM VC class. This problem is resolved in Release 12.1(26)E4. (CSCeg83164)
- Port 1/7 ingress traffic is dropped if the egress port is on an OSM. This problem is resolved in Release 12.1(26)E4. (CSCeh05310)

Resolved OSM Caveats in Release 12.1(26)E3

None.

Resolved OSM Caveats in Release 12.1(26)E2

None.

Resolved OSM Caveats in Release 12.1(26)E1

- When parallel EoMPLS VC links are connected to the next hop through an Ethernet switch, the EoMPLS VCs drop traffic if they become unstable. This problem is resolved in Release 12.1(26)E1. (CSCeh16928)
- When supporting VPN and MPLS traffic, an OSM-2+4GE-WAN+ might reset if the interface to which it is connected shuts down. This problem is resolved in Release 12.1(26)E1. (CSCsa59568)

Resolved OSM Caveats in Release 12.1(26)E

- On an OSM-1CHOC12/T1-SI, when modifying a configuration from E3 to E1, the newly configured E1s stay down. This problem is resolved in Release 12.1(26)E. (CSCsa43724)
- In rare situations, a reload might occur if you modify an existing PVC. This problem is resolved in Release 12.1(26)E. (CSCed29265)
- With QoS configured on an OSM multilink interface, a reload might occur if the multilink interface becomes unstable. This problem is resolved in Release 12.1(26)E. (CSCsa44933)
- On a channelized OSM, a reload might occur if you remove a service policy from a multilink interface while it is down. This problem is resolved in Release 12.1(26)E. (CSCsa43246)
- On a channelized OSM, a reload might occur if there is an input service policy on an unstable multilink interface. This problem is resolved in Release 12.1(26)E. (CSCsa43242)
- On a channelized OSM, after a reload, the clock source might be incorrect. This problem is resolved in Release 12.1(26)E. (CSCef79815)
- On a channelized OSM, after a reload, some of the links in a multilink interface might not come up. This problem is resolved in Release 12.1(26)E. (CSCef78798)
- On a channelized OSM, after you enter the **aps force** command to change the status of an automatic protection switching (APS) interface from protect to working, IP routing is not notified of the status change. This problem is resolved in Release 12.1(26)E. (CSCef45881)
- The SNMP ifHCOutOctets and ifHCInOctets MIB objects always have a value of zero. This problem is resolved in Release 12.1(26)E. (CSCef42133)
- Hierarchical service policies do not work correctly on physical interfaces configured for Frame Relay encapsulation when subinterfaces are also configured. This problem is resolved in Release 12.1(26)E. (CSCee38898)

- In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment, incorrect tags might be imposed after a route flaps. This problem is resolved in Release 12.1(26)E. (CSCec31162)
- Changing the MTU size on a port might not change the MPLS MTU size. This problem is resolved in Release 12.1(26)E. (CSCed17226, CSCed33822)
- With OSM serial interfaces configured, you might see these messages:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 65535
-Process= "<interrupt level>", ipl= 1
-Traceback= 4021F160 402E3BCC 40E9CA28 40E90E68 402D545C 40294A0C
```

  This problem is resolved in Release 12.1(26)E. (CSCed82736)
- If you enter the **encapsulation dot1q** *vlan_id* command on an OSM Gigabit Ethernet WAN port with the VLAN ID of an internal VLAN, the port does not forward traffic. This problem is resolved in Release 12.1(26)E. (CSCef08790)
- A reload might occur if you configure Point-to-Point Protocol (PPP) and High Level Data Link Control (HDLC) on a channelized OSM. This problem is resolved in Release 12.1(26)E. (CSCef32629)
- If you configure 802.1Q tunneling on a LAN port and 802.1Q-tunnel bridging on an OSM-2OC12-ATM-SI+ subinterface, the OSM might reload. This problem is resolved in Release 12.1(26)E. (CSCef35398)
- When any interface on an OSM-12CT3/T1 goes down, traffic to a directly connected router might experience high latency. This problem is resolved in Release 12.1(26)E. (CSCef47466)
- When deleting and re-adding channels on an OSM-12CT3/T1 T1 interface, the SNMP ifindex disappears. This problem is resolved in Release 12.1(26)E. (CSCef70298)
- When configured as an 802.1q trunk port, the Layer 2 LAN ports on OSMs do not allow for the 802.1q tag when counting packets as giants. This problem is resolved in Release 12.1(26)E. (CSCef74227)

Release 12.1(23)E and Rebuilds

- General Caveats, page 159
- FlexWAN Module Caveats, page 169
- Service Module Caveats, page 170
- OSM Caveats, page 171

Note The caveat lists for Release 12.1(23)E are still being updated.

General Caveats

- Open General Caveats in Release 12.1(23)E4, page 160
- Resolved General Caveats in Release 12.1(23)E4, page 160
- Resolved General Caveats in Release 12.1(23)E3, page 160
- Resolved General Caveats in Release 12.1(23)E2, page 161
- Resolved General Caveats in Release 12.1(23)E1, page 162

- Resolved General Caveats in Release 12.1(23)E, page 163

Open General Caveats in Release 12.1(23)E4

None.

Resolved General Caveats in Release 12.1(23)E4

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

  This problem is resolved in Release 12.1(23)E4. (CSCei61732)
- Receipt of a Border Gateway Protocol (BGP) Autonomous System (AS) path with a length that is equal to or greater than 255 might reset the BGP session. This problem is resolved in Release 12.1(23)E4. (CSCeh13489)

Resolved General Caveats in Release 12.1(23)E3

- Policing might not be accurate for packets smaller than 82 bytes. This problem is resolved in Release 12.1(23)E3. (CSCee78451)
- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in Release 12.1(23)E3. (CSCef44225, CSCef44699, CSCef60659, CSCsa59600)

Resolved General Caveats in Release 12.1(23)E2

- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

  Cisco has made free software available to address this problem.

  For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

  This problem is resolved in Release 12.1(23)E2. (CSCee67450)
- After you enter the **squeeze** command for a 32-MB bootflash device, you cannot write any files to the bootflash. This problem is resolved in Release 12.1(23)E2. (CSCef15418)
- Traffic is routed in software when it uses a static ARP entry with an IP route that has a destination that is a local interface instead of an IP next-hop address. A static ARP entry created after a dynamic ARP has been learned prevents the updating of the dynamic ARP entry. This problem is resolved in Release 12.1(23)E2. (CSCee49121)
- A reload might occur if the order-dependent ACL merge (ODM) algorithm fails. This problem is resolved in Release 12.1(23)E2. (CSCin83455)
- After a reload, or following a switchover to a redundant supervisor engine, service policies that were attached to Layer 3 VLAN interfaces are missing. This problem is resolved in Release 12.1(23)E2. (CSCin80578)
- When the number of routing table entries exceeds the capacity of the hardware-forwarding information base (FIB), the routing table entry for a default route might change so that traffic is dropped instead of forwarded. This problem is resolved in Release 12.1(23)E2. (CSCin78197)
- Over an SSHv2 connection, the output from a command that displays many lines of text pauses until you press a key. This problem is resolved in Release 12.1(23)E2. (CSCef61978)
- In rare situations, a reload might occur if you enter the **show mls qos ip** command. This problem is resolved in Release 12.1(23)E2. (CSCef50318)
- With a Supervisor Engine 1, copying files with TFTP takes longer than usual because many corrected errors occur during the copy process. This problem is resolved in Release 12.1(23)E2. (CSCef26370)
- For QoS filtering, extended ACLs that are configured to match DSCP parse 7 bits of the ToS byte instead of 6 bits. This problem is resolved in Release 12.1(23)E2. (CSCec86976)
- In rare situations, the MSFC might stop responding to received traffic. This problem is resolved in Release 12.1(23)E2. (CSCef85654)
- Occasionally, these modules might lose the ability to communicate over the Ethernet Out of Band Channel (EOBC) and reset:
  - WS-X6416-GBIC
  - WS-X6348-RJ-45
  - WS-X6148-RJ-45

- WS-X6348-RJ-21
- WS-X6148-RJ-21
- WS-X6316-GE-TX
- WS-X6324-100FX
- WS-X6416-GE-MT
- WS-X6024-10FL-MT

This problem is resolved in Release 12.1(23)E2. (CSCef23843)

Resolved General Caveats in Release 12.1(23)E1

- SNMP traps are sent for every Internet Key Exchange (IKE) timeout and rekey but not for every IPsec timeout and rekey. This situation might generate many false alerts that an IKE tunnel is down when the IKE tunnel is torn down but immediately rebuilt. Releases where CSCee91044 is resolved do not send SNMP traps that are sent for normal IKE operation. This problem is resolved in Release 12.1(23)E1. (CSCee91044)
- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

  The Advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

  This problem is resolved in Release 12.1(23)E1. (CSCef46191)
- In an MPLS VPN provider edge (PE) configuration, for prefixes with multiple paths, some of which are on an OIRed switching module, the local label for a prefix in the label forwarding information base (LFIB) might be different from the local label allocated by the Label Distribution Protocol (LDP). To display the LFIB local label, enter the **show mpls forwarding prefix** command. To display the LDP-allocated local label, enter the **show mpls ldp binding prefix mask length** command. This problem is resolved in Release 12.1(23)E1. (CSCee72857)
- After you enter a **shutdown** command on a physical ATM interface, ATM subinterfaces configured on the physical ATM interface are displayed as “down” instead of “administratively down.” This problem is resolved in Release 12.1(23)E1. (CSCea92873)
- Configuring an extended Border Gateway Protocol (BGP) community-list statement with any illegal regular expression pattern might cause a reload. This problem is resolved in Release 12.1(23)E1. (CSCdx71842)
- A memory leak might occur with Cisco IOS firewall authentication proxy configured. This problem is resolved in Release 12.1(23)E1. (CSCef14971)

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in Release 12.1(23)E1. (CSCed78149)

- With multicast support configured on a Supervisor Engine 2, VACLs do not capture traffic for RSPAN. This problem is resolved in Release 12.1(23)E1. (CSCef07017)

Resolved General Caveats in Release 12.1(23)E

- Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  This problem is resolved in Release 12.1(23)E (CSCec71950)

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust

resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

This problem is resolved in Release 12.1(23)E. (CSCed65285)

- A reload might occur if you apply egress WAN QoS features to an ingress WAN interface. This problem is resolved in Release 12.1(23)E. (CSCin77116)
- If you create a new SNMP probe (for example, index $PROBE_ID) in the CREATE_AND_WAIT state, SNMP probes that have index numbers that are greater than $PROBE_ID are not shown in the output of the **show rtr configuration** and **show rtr operation-state** commands. This problem is resolved in Release 12.1(23)E. (CSCin63066)
- If you configure the RPR redundancy mode and Cisco IOS SLB, switchover to a redundant supervisor engine might fail and you might not be able to access the active supervisor engine. This problem is resolved in Release 12.1(23)E. (CSCee70320)
- When an ARP entry is internally rearranged during the ARP table lookup process and when a race condition occurs between the ARP table lookup process and other processes, a reload might occur when the ARP entry ages out. This problem is resolved in Release 12.1(23)E. (CSCea70296)
- UDP port 1985 is open. This problem is resolved in Release 12.1(23)E. (CSCdt64533)
- In rare situations, a reload might occur when the FIB TCAM goes in and out of the FIB TCAM exception condition. This problem is resolved in Release 12.1(23)E. (CSCin75706)
- Traffic loss might occur if you configure a loopback interface with an IP address that is already in use elsewhere in the network and there are multiple paths to the prefix. This problem is resolved in Release 12.1(23)E. (CSCee85152)
- Boot failure might occur when there are more than 256 different policy maps attached as service policies. This problem is resolved in Release 12.1(23)E. (CSCee24349)
- A small (approximately 180 bytes) memory leak occurs when you delete a logical interface. This problem is resolved in Release 12.1(23)E. (CSCee05413)
- Receiving CDP packets with a host name that is 256 or more characters long might cause a memory leak in the CDP process. This problem is resolved in Release 12.1(23)E. (CSCin67568)
- Following switchover to a redundant supervisor engine, any EtherChannels on the newly active supervisor engine are not active and the newly redundant supervisor engine does not enter the standby state. This problem is resolved in Release 12.1(23)E. (CSCee44248)
- Traffic through a port-channel interface that has a Cisco IOS ACL configured might be dropped or switched in software after a reload or after switchover to a redundant supervisor engine or after you enter **shutdown** and **no shutdown** interface commands on a member port. This problem is resolved in Release 12.1(23)E. (CSCee21772)
- After you configure a tunnel to support DECnet with assigned DECnet cost and then delete the tunnel configuration, a reload might occur if you disable DECnet routing. This problem is resolved in Release 12.1(23)E. (CSCed88563)
- If you change the STP root bridge, a Layer 2 loop might exist very briefly. This problem is resolved in Release 12.1(23)E. (CSCed85411)

- When you use local-proxy-arp and HSRP, the active MSFC could respond to ARP requests with the BIA MAC address and the redundant MSFC might keep cached ARP entries that should have been deleted. This problem is resolved in Release 12.1(23)E. (CSCed72287)
- After Cisco IOS ACLs have been updated dynamically or after responding dynamically to an IDS signature, a reload might occur following attempts to access a low memory address. This problem is resolved in Release 12.1(23)E. (CSCed35253)
- When you configure BGP peergroups, spurious memory access messages are displayed. This problem is resolved in Release 12.1(23)E. (CSCec78347)
- If the FIB TCAM is full, a memory leak or a reload might occur or you might observe high supervisor engine utilization. This problem is resolved in Release 12.1(23)E. (CSCeb85827, CSCeb29888, CSCec14802, CSCec42634, CSCed58661, CSCee00311, CSCee22821)
- With MD5 password encryption configured, the software does not correctly verify that all configured TCP options can be sent in a TCP packet, which can cause this message to be displayed:

  ```
  %TCP-6-TOOBIG: Tty0, too many bytes of options (44)
  ```

  This problem is resolved in Release 12.1(23)E. (CSCeb07106)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in Release 12.1(23)E. (CSCed93836, CSCdz84583)
- Many memory allocation failure (MALLOCFAIL) messages might occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
  Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  This problem is resolved in Release 12.1(23)E. (CSCdz32659)
- With both static and dynamic Port Address Translation (PAT) configured and if the **ip nat pool** *inside_pool_name* command has been entered for only one IP address, the IP addresses that are used for overloading might be used as one-to-one translations. This problem is resolved in Release 12.1(23)E. (CSCdx19396)

- There is no response to SNMP requests and memory use increases until tracebacks occur. This problem is resolved in Release 12.1(23)E. (CSCed52841)
- With certain configurations, a reload might occur when you enter the **show cdp entry * protocol** command. This problem is resolved in Release 12.1(23)E. (CSCed40563)
- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

  This problem is resolved in Release 12.1(23)E. (CSCed21717)
- Traffic loss might occur on fabric-enabled modules when there are frequent online insertion and removals (OIRs). This problem is resolved in Release 12.1(23)E. (CSCee44496, CSCee48403, CSCee78766)
- In a release where caveat CSCec55429 is resolved, after a number of Web Cache Communication Protocol (WCCP) “cache lost” and “cache found” events have occurred for all the caches in a service group, spurious memory accesses might occur, the addition and deletion of WCCP services might fail, and the **show ip wccp** command displays the WCCP service, but the output of the **show ip wccp** *service_number* command does not show the WCCP service. This problem is resolved in Release 12.1(23)E. (CSCuk50878)
- A reload might occur when traffic enters a port configured with the **switchport protocol ip auto** command. This problem is resolved in Release 12.1(23)E. (CSCin77984)
- If there are more than 50 files on the flash card, access from CiscoView Device Manager (CVDM) might cause a reload. This problem is resolved in Release 12.1(23)E. (CSCef07965)
- Occasionally, CEF incorrectly perceives the state of an active interface and does not forward traffic to what it perceives as an inactive interface. This problem is resolved in Release 12.1(23)E. (CSCdt38401)
- With a PFC2 and GRE tunnel traffic, the “do not fragment” (DF) bit might not be copied correctly and the time-to-live (TTL) count might not be decremented correctly. This problem is resolved in Release 12.1(23)E. (CSCuk49481)
- In a topology where MAC addresses move frequently (for example, as the result of wireless access through various access points) and where there are STP topology change notices (TCNs), EtherChannels with interfaces on different distributed forwarding card (DFC)-equipped switching modules might drop traffic. This problem is resolved in Release 12.1(23)E. (CSCee83733)
- SNMP returns a null value for the server load balancing (SLB) real server name. This problem is resolved in Release 12.1(23)E. (CSCee60121)
- After a reload, the **no diagnostic cns publish** and **logging event link-status** commands revert to their defaults in the running-config file, and some **switchport mode access** commands might be missing from the running-config file. This problem is resolved in Release 12.1(23)E. (CSCee53998)
- 802.1X port-based authentication does not support receipt of a VLAN ID in the tunnel attribute from a RADIUS server. The tunnel attribute from a RADIUS server is seen as a VLAN name. This problem is resolved in Release 12.1(23)E. (CSCee51684)

- In a release where caveat CSCeb06811 is resolved and with STP loop guard configured, two ports connected together might incorrectly stay in the STP loopguard loop-inconsistent state. This problem is resolved in Release 12.1(23)E. (CSCee45170)
- While traffic is flowing, CPU utilization might increase to a very high level if you reconfigure an EtherChannel from Layer 3 to Layer 2 and configure a Layer 3 VLAN interface for the EtherChannel. This problem is resolved in Release 12.1(23)E. (CSCee41100)
- Traffic might be lost when communication fails between the supervisor engine and the MSFC. This problem is resolved in Release 12.1(23)E: an intentional reload occurs when communication fails between the supervisor engine and the MSFC. (CSCee39004)
- With very large flows, the NetFlow Data Export (NDE) byte counts might be incorrect (NDE packet counts remain correct). This problem is resolved in Release 12.1(23)E. (CSCee23058)
- If you enter the **mls ip multicast non-rpf netflow** and **mls ip multicast consistency-check** commands, the **show mls ip multicast consistency-check** command displays "mdb missed for a shortcut" for non-RPF traffic, because non-RPF traffic has no (S,G) entry in the multicast routing table. This problem is resolved in Release 12.1(23)E. (CSCee22471)
- Following a Route Processor Redundancy Plus (RPR+) mode switchover, if you enter the **reload** command, you are prompted to save the configuration when the configuration has not been changed. This problem is resolved in Release 12.1(23)E. (CSCee05637)
- When you configure Network Based Application Recognition (NBAR) on a LAN port, there is no message that the NBAR traffic is processed in software on the MSFC. This problem is resolved in Release 12.1(23)E. (CSCed90255)
- SNMP access of the CISCO-SWITCH-ENGINE-MIB might cause tracebacks. This problem is resolved in Release 12.1(23)E. (CSCed85167)
- The VLAN translation feature does not work on WS-X6816-GBIC modules. This problem is resolved in Release 12.1(23)E. (CSCed73700)
- You cannot disable the power reserved for empty slots. This problem is resolved in Release 12.1(23)E: you can enter the **no power enable module** command for an empty slot. (CSCed56651)
- A VLAN interface configured on a VLAN that is carrying Layer 2 protocol tunneling traffic processes untagged CDP frames and displays the CDP-frame-source devices as CDP neighbors. This problem is resolved in Release 12.1(23)E. (CSCed55283)
- Cisco IOS software does not prevent simultaneous **erase nvram:** and **write memory** commands from different Telnet or console sessions. This problem is resolved in Release 12.1(23)E. (CSCea20169)
- No CDP packets are received if you enter the **dlsw ethernet redundancy-enable** command on a VLAN interface. This problem is resolved in Release 12.1(23)E. (CSCee39240)
- You might see these messages with a large ARP table and heavy ARP traffic:

```
%SYS-3-CPUHOG: Task ran for 2376 msec (6/4), process = ARP Input, PC =40292C18.
-Traceback= 40292C20 401D8624 401D8610
%SYS-3-CPUHOG: Task ran for 2160 msec (18/13), process = ARP Input, PC = 40292C18.
-Traceback= 40292C20 401D8624 401D8610
```

  This problem is resolved in Release 12.1(23)E. (CSCed28402)
- The BGP **set community none** command does not work; prefixes are not advertised to external peers. This problem is resolved in Release 12.1(23)E. (CSCeb69972)
- Spurious memory accesses might occur if you remove DECnet configuration commands associated with a tunnel interface. This problem is resolved in Release 12.1(23)E. (CSCee88936)

- In releases where caveat CSCdy36604 is resolved, you cannot use SNMP to retrieve dot1dBase group data on VLANs where the spanning tree protocol is not enabled. This problem is resolved in Release 12.1(23)E. (CSCee39798)
- HSRP tracking might incorrectly track two instances of the same interface, stating that one instance is down while the other is up. This situation causes the HSRP priority to be decremented by 10. This problem is resolved in Release 12.1(23)E. (CSCed95701)
- When the Multicast Border Gateway Protocol (MBGP) table has an invalid entry for the originating Rendezvous Point (RP), Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages from an interior Border Gateway Protocol (iBGP) peer might not get populated because of RPF check failures. This problem is resolved in Release 12.1(23)E. (CSCed68093)
- When an OSPF external route has a forwarding address with a next hop address in the routing table, the next hop address does not get updated in the type 5 link-state advertisement (LSA) when the forwarding address gets a more specific entry in the routing table with a different next hop address. This problem is resolved in Release 12.1(23)E. (CSCed59370)
- Configuration of fair queuing fails on virtual-template interfaces. This problem is resolved in Release 12.1(23)E. (CSCed54330)
- You might see high CPU utilization if you enter the **logging synchronous** command. This problem is resolved in Release 12.1(23)E. (CSCed16920)
- If you enter the **show tech-support** command, you might see "%SCHED-2-NOTWATCHTIMER" and "%SCHED-3-STILLWATCHINGT" messages. This problem is resolved in Release 12.1(23)E. (CSCec67602)
- In a PIM dense mode environment, a forwarding interface might be pruned because join messages are delayed. This problem is resolved in Release 12.1(23)E. (CSCec37022)
- In releases where caveat CSCdz18109 is resolved, you cannot ping or make Telnet connections to outside local addresses from the NAT router with "ip nat outside source ..." translations configured. This problem is resolved in Release 12.1(23)E. (CSCec33530)
- With the **distribute-list** command configured to filter redistributed EIGRP static routes, when you configure the filtering to permit additional static routes, the routes are not redistributed. This problem is resolved in Release 12.1(23)E. (CSCdz21986)
- The **show interface summary** command might truncate some of the final characters of an interface name. This problem is resolved in Release 12.1(23)E. (CSCdx62060)
- If you power-cycle redundant SFMs, DFC-equipped switching modules might not come back online. This problem is resolved in Release 12.1(23)E. (CSCin70599)
- When a Multicast Source Discovery Protocol (MSDP)-enabled rendezvous point (RP) for a multicast group fails and an incoming (*,G) join message is received, the RP does not build an (S,G) state from its Source-Active (SA) cache when it should do so. Depending on the topology and if a Shortest Path Tree (SPT) threshold is configured as infinite, this situation might result in a multicast forwarding interruption of up to 2 minutes. This problem is resolved in Release 12.1(23)E. (CSCee89438)
- A reload might occur if the output of a **show** command is left at the "More" prompt for an extended period, and you attempt to resume display of the command output. This problem is resolved in Release 12.1(23)E. (CSCee89232)
- For ACEs that match on DSCP, 7 bits instead of 6 bits are programmed into the ACL TCAM. This problem is resolved in Release 12.1(23)E. (CSCee39170)
- OSPF area border routers (ABRs) might continue to generate summary link-state advertisements (LSAs) for obsolete nonbackbone intra-area routes. This problem is resolved in Release 12.1(23)E. (CSCee36622)

- With a switch fabric module (SFM), some modules might stop egressing traffic. This problem is resolved in Release 12.1(23)E. (CSCee08015)
- A reload might follow this message:

  ```
  %C6KERRDETECT-SP-2-SUPSWO: Supervisor card switchover due to unrecoverable errors
  detected, Reason: Failed In-band Path
  ```

  This problem is resolved in Release 12.1(23)E. (CSCee01297)
- WCCP-redirected packets that have no next hop ARP cache entry are process-switched to generate an ARP request. Because the WCCP redirection causes no ARP requests to be sent, the ARP cache is never populated for the next hop, and subsequent WCCP-redirected packets continue to be process switched. This problem is resolved in Release 12.1(23)E. (CSCed92290)
- When the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured, the withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table. This problem is resolved in Release 12.1(23)E. (CSCed60800)
- After a few days of running time, the **show environment temperature** command does not display current values. This problem is resolved in Release 12.1(23)E. (CSCed49423)
- Some packet loss might occur when a host sends and receives both bridged traffic and routed traffic through a Layer 2 switch that connects through a nontrunking cross-DFC EtherChannel to a Supervisor Engine 2. This problem is resolved in Release 12.1(23)E. (CSCed06744)
- Under heavy traffic conditions, online insertion and removal (OIR) of a switch fabric module or OIR of a nonfabric-enabled module might cause OSMs to stop forwarding traffic. This problem is resolved in Release 12.1(23)E. (CSCec49269)
- The time-to-live value (TTL value) might not be decremented correctly in tunnel traffic. This problem is resolved in Release 12.1(23)E. (CSCea77189)
- The Multicast Broader Gateway Protocol (MBGP) default route is advertised as 0.0.0.0/0 to a Protocol Independent Multicast (PIM) neighbor, but the MBGP default route is not considered for a multicast Reverse Path Forwarding (RPF) check on the router. This problem is resolved in Release 12.1(23)E. (CSCdy59996)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(23)E4, page 169
- Resolved FlexWAN Module Caveats in Release 12.1(23)E4, page 169
- Resolved FlexWAN Module Caveats in Release 12.1(23)E3, page 170
- Resolved FlexWAN Module Caveats in Release 12.1(23)E2, page 170
- Resolved FlexWAN Module Caveats in Release 12.1(23)E1, page 170
- Resolved FlexWAN Module Caveats in Release 12.1(23)E, page 170

Open FlexWAN Module Caveats in Release 12.1(23)E4

None.

Resolved FlexWAN Module Caveats in Release 12.1(23)E4

None.

Resolved FlexWAN Module Caveats in Release 12.1(23)E3

None.

Resolved FlexWAN Module Caveats in Release 12.1(23)E2

None.

Resolved FlexWAN Module Caveats in Release 12.1(23)E1

- Serial interfaces on a PA-MC-8TE1+ port adapter that are configured as part of a channel group continue to process packets when the interface is in the "admindown" state. The counters in the output of the **show interfaces serial** command might increment when the serial interface is shut down. This problem is resolved in Release 12.1(23)E1. (CSCin78325)

Resolved FlexWAN Module Caveats in Release 12.1(23)E

- PA-A3-8T1IMA and PA-A3-8E1IMA port-adapter interfaces generate repeated "changed state to up" messages without corresponding "changed state to down" messages. This problem is resolved in Release 12.1(23)E. (CSCin05262)
- EIGRP neighbors flap and output traffic is dropped when traffic on a PA-A3-8T1IMA or PA-A3-8E1IMA port-adapter interface is 40 percent or more of the non-real time variable bit rate (VBR-nrt) parameter. This problem is resolved in Release 12.1(23)E. (CSCee50948)
- A response time reporter (RTR) probe does not report input or output packets for serial interfaces of PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters. This problem is resolved in Release 12.1(23)E. (CSCee82681)
- You might see CWAN_RP-3-SEMAHOG messages and tracebacks or CMDTIMEOUT messages and tracebacks. This problem is resolved in Release 12.1(23)E. (CSCin54713)
- VACL capture does not support PPP multilinks on the FlexWAN module. This problem is resolved in Release 12.1(23)E. (CSCee07996)
- In releases where CSCdz75507 is resolved, you cannot configure fall-back bridging on any subinterface under a physical interface where MPLS is configured on another subinterface. This problem is resolved for Frame Relay interfaces in Release 12.1(23)E. (CSCee00239; also see resolved caveat CSCeb87433)
- A reload might occur if you do the following on a FlexWAN module interface:
  - Attach an egress queueing policy
  - Attach an ingress policy that uses the same policy-map class
  - Remove the ingress policy
  - Update a queueing feature in the egress policy

  This problem is resolved in Release 12.1(23)E. (CSCee40863)
- With multilink PPP configured, fragmentation might cause spurious accesses and tracebacks. This problem is resolved in Release 12.1(23)E. (CSCed65436)

Service Module Caveats

- Open Service Module Caveats in Release 12.1(23)E4, page 171
- Resolved Service Module Caveats in Release 12.1(23)E4, page 171

- Resolved Service Module Caveats in Release 12.1(23)E3, page 171
- Resolved Service Module Caveats in Release 12.1(23)E2, page 171
- Resolved Service Module Caveats in Release 12.1(23)E1, page 171
- Resolved Service Module Caveats in Release 12.1(23)E, page 171

Open Service Module Caveats in Release 12.1(23)E4

None.

Resolved Service Module Caveats in Release 12.1(23)E4

None.

Resolved Service Module Caveats in Release 12.1(23)E3

None.

Resolved Service Module Caveats in Release 12.1(23)E2

- If you reset a WS-X6066-SLB-APC Content Switching Module (CSM), other modules might also reset. This problem is resolved in Release 12.1(23)E2. (CSCed25505)

Resolved Service Module Caveats in Release 12.1(23)E1

None.

Resolved Service Module Caveats in Release 12.1(23)E

- The SNMP slbStickyObjectTableEntry MIB object is not supported. This problem is resolved in Release 12.1(23)E. (CSCef05643)
- If a CSM server farm is configured with a real server name instead of a real server IP address, SNMP does not retrieve and display the IP address of the real server in the CISCO-SLB-MIB server table. This problem is resolved in Release 12.1(23)E. (CSCed84042)
- The internal EtherChannel that connects the WS-X6066-SLB-APC incorrectly does not trust DSCP, which sets DSCP to zero in all packets from the WS-X6066-SLB-APC when QoS is enabled. This problem is resolved in Release 12.1(23)E. (CSCec27686)

OSM Caveats

- Open OSM Caveats in Release 12.1(23)E4, page 171
- Resolved OSM Caveats in Release 12.1(23)E4, page 172
- Resolved OSM Caveats in Release 12.1(23)E3, page 172
- Resolved OSM Caveats in Release 12.1(23)E2, page 172
- Resolved OSM Caveats in Release 12.1(23)E1, page 172
- Resolved OSM Caveats in Release 12.1(23)E, page 172

Open OSM Caveats in Release 12.1(23)E4

None.

Resolved OSM Caveats in Release 12.1(23)E4

None.

Resolved OSM Caveats in Release 12.1(23)E3

None.

Resolved OSM Caveats in Release 12.1(23)E2

- If you configure 802.1Q tunneling on a LAN port and 802.1Q-tunnel bridging on an OSM-2OC12-ATM-SI+ subinterface, the OSM might reload. This problem is resolved in Release 12.1(23)E2. (CSCef35398)

Resolved OSM Caveats in Release 12.1(23)E1

- A reload might occur if you configure Point-to-Point Protocol (PPP) and High Level Data Link Control (HDLC) on a channelized OSM. This problem is resolved in Release 12.1(23)E1. (CSCef32629)

Resolved OSM Caveats in Release 12.1(23)E

- You might see semaphore hog messages with a large Bridging of Routed Encapsulations (BRE) configuration. This problem is resolved in Release 12.1(23)E. (CSCef07770)
- OSM-1CHOC12/T1-SI T1 interfaces that have path coding violations (PCVs) might cause erroneous Layer 1 errors to be displayed for other T1 interfaces. This problem is resolved in Release 12.1(23)E. (CSCed86486)
- Traffic might be dropped if you enter the **no ip cef** global configuration command. This problem is resolved in Release 12.1(23)E. (CSCin40371)
- An OSM might be reset following an online insertion and removal (OIR) of a Switch Fabric Module (SFM) or during periods of heavy traffic. This problem is resolved in Release 12.1(23)E. (CSCin37112)
- A reload might occur if you enter a **show controllers sonet** command with an invalid number for a T1 interface on a OSM-1CHOC12/T1-SI or OSM-12CT3/T1 module. This problem is resolved in Release 12.1(23)E. (CSCee50911)
- OSM-1CHOC12 modules become unresponsive and are power cycled. This problem is resolved in Release 12.1(23)E. (CSCee45508)
- An OSM-12CT3/T1 module with an E1 channel group configured is powered down. This problem is resolved in Release 12.1(23)E. (CSCee42278)
- If you have an input service policy that is configured only to police attached to an OSM interface and you do not have an output service policy attached to the OSM interface and you OIR another module, the OSM might reset. This problem is resolved in Release 12.1(23)E. (CSCee42074)
- Multicast 127-byte UDP packets that egress from OSM-2OC12-POS interfaces have invalid checksums. This problem is resolved in Release 12.1(23)E. (CSCec72798)
- OSM ATM interfaces do not support the SNMP lowerLayerDown value defined in RFC 2863. This problem is resolved in Release 12.1(23)E. (CSCee56269)
- OSM ATM interfaces do not support unspecified bit rate plus (UBR+) virtual circuit (VC) class maps, but you can apply UBR+ VC class maps to VC subinterfaces. This problem is resolved in Release 12.1(23)E. (CSCec31381)

- With high CPU utilization and line-rate traffic, byte counters on OC-48 interfaces might be wrong. This problem is resolved in Release 12.1(23)E. (CSCee84887)
- OSM-2+4GE-WAN+ ports do not automatically adjust the MTU size to accommodate tagged traffic. Ingress tagged packets destined for the MSFC are dropped if the packet size is larger than the ingress interface MTU size. This problem is resolved in Release 12.1(23)E. (CSCee59667)
- OSM interface byte counts might be incorrect after a few hours of traffic handling. High traffic levels on OC-48 interfaces might produce incorrect byte counts. This problem is resolved in Release 12.1(23)E. (CSCee55056)
- Traffic loss might occur on OSMs when there are frequent OIRs. This problem is resolved in Release 12.1(23)E. (CSCee54642)
- The interfaces on an OSM-2+4GE-WAN+ module might be reported as administratively “up/up” when there is no GBIC installed. This problem is resolved in Release 12.1(23)E. (CSCee35867)
- The Gigabit Ethernet LAN ports on a OSM-2+4GE-WAN+ module might be reported as administratively “up/up” when there is a GBIC installed but no cable attached. This problem is resolved in Release 12.1(23)E. (CSCee01868)
- Occasionally, OSM-2+4GE-WAN+ module interfaces do not pass traffic after a reload or OIR. This problem is resolved in Release 12.1(23)E. (CSCed83227)

Release 12.1(22)E and Rebuilds

- General Caveats, page 173
- FlexWAN Module Caveats, page 187
- Service Module Caveats, page 189
- OSM Caveats, page 190

General Caveats

- Open General Caveats in Release 12.1(22)E6, page 173
- Resolved General Caveats in Release 12.1(22)E6, page 174
- Resolved General Caveats in Release 12.1(22)E5, page 174
- Resolved General Caveats in Release 12.1(22)E4, page 174
- Resolved General Caveats in Release 12.1(22)E3, page 175
- Resolved General Caveats in Release 12.1(22)E2, page 177
- Resolved General Caveats in Release 12.1(22)E1, page 178
- Resolved General Caveats in Release 12.1(22)E, page 179

Open General Caveats in Release 12.1(22)E6

- A reload might follow this message:

  ```
  %C6KERRDETECT-SP-2-SUPSWO: Supervisor card switchover due to unrecoverable errors
  detected, Reason: Failed In-band Path
  ```

  This problem is resolved in Release 12.1(23)E. (CSCee01297)

Resolved General Caveats in Release 12.1(22)E6

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in Release 12.1(22)E6. (CSCef44225, CSCef44699, CSCef60659, CSCsa59600)

Resolved General Caveats in Release 12.1(22)E5

- For QoS filtering, extended ACLs that are configured to match DSCP parse 7 bits of the ToS byte instead of 6 bits. This problem is resolved in Release 12.1(22)E5. (CSCec86976)

Resolved General Caveats in Release 12.1(22)E4

- With a Supervisor Engine 1 and an MSFC2, when the TCAM mask utilization reaches approximately 50 percent, you might see these TCAM mask exception messages:

  ```
  00:11:17: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
  00:11:17: %QM-SP-4-WARNING: TCAM request replace [lkup=2] status:1
  00:11:17: SP: TCAM ASSERT FAILURE: label_alloc_tbl[label].num_if_using[lookup_type]
  != 0: ../const/native-sp/tcam_label.c: 1379
  00:11:17: SP: -Traceback= 603C1090 603ACAE0 603AA018 603B7F38 603B8994 6039CE5C
  603A53B8 6039D110 6039D254 6039D360 6039D6B4 6039D8E0 600FA6CC 600FA6B8
  ```

  This problem is resolved in Release 12.1(22)E4. (CSCef73019)

- In IP packets with the IP options field populated, the IP type-of-service (ToS) byte might be truncated to a 3-bit long field. This problem deletes 3 bits of the 6-bit DSCP value and causes incorrect QoS operation. This problem is resolved in Release 12.1(22)E4. (CSCed93264)
- A reload might occur if the order-dependent ACL merge (ODM) algorithm fails. This problem is resolved in Release 12.1(22)E4. (CSCin83455)

- For ACEs that match on DSCP, 7 bits instead of 6 bits are programmed into the ACL TCAM. This problem is resolved in Release 12.1(22)E4. (CSCee39170)

Resolved General Caveats in Release 12.1(22)E3

- SNMP traps are sent for every Internet Key Exchange (IKE) timeout and rekey but not for every IPsec timeout and rekey. This situation might generate many false alerts that an IKE tunnel is down when the IKE tunnel is torn down but immediately rebuilt. Releases where CSCee91044 is resolved do not send SNMP traps that are sent for normal IKE operation. This problem is resolved in Release 12.1(22)E3. (CSCee91044)
- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

  Cisco has made free software available to address this problem.

  For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

  This problem is resolved in Release 12.1(22)E3. (CSCee67450)
- In rare situations, the MSFC might stop responding to received traffic. This problem is resolved in Release 12.1(22)E3. (CSCef85654)
- In a release where caveat CSCec55429 is resolved, after a number of WCCP "cache lost" and "cache found" events have occurred for all the caches in a service group, spurious memory accesses might occur, the addition and deletion of WCCP services might fail, and the **show ip wccp** command displays the WCCP service, but the output of the **show ip wccp** *service_number* command does not show the WCCP service. This problem is resolved in Release 12.1(22)E3. (CSCuk50878)
- With both static and dynamic Port Address Translation (PAT) configured and if the **ip nat pool** *inside_pool_name* command has been entered for only one IP address, the IP addresses that are used for overloading might be used as one-to-one translations. This problem is resolved in Release 12.1(22)E3. (CSCdx19396)
- With MD5 password encryption configured, the software does not correctly verify that all configured TCP options can be sent in a TCP packet, which can cause this message to be displayed:

  ```
  %TCP-6-TOOBIG: Tty0, too many bytes of options (44)
  ```

  This problem is resolved in Release 12.1(22)E3. (CSCeb07106)
- Under heavy traffic conditions, online insertion and removal (OIR) of a switch fabric module or OIR of a nonfabric-enabled module might cause OSMs to stop forwarding traffic. This problem is resolved in Release 12.1(22)E3. (CSCec49269)
- When you configure BGP peergroups, spurious memory access messages are displayed. This problem is resolved in Release 12.1(22)E3. (CSCec78347)
- You might see high CPU utilization if you enter the **logging synchronous** command. This problem is resolved in Release 12.1(22)E3. (CSCed16920)

- When an OSPF external route has a forwarding address with a next hop address in the routing table, the next hop address does not get updated in the type 5 link-state advertisement (LSA) when the forwarding address gets a more specific entry in the routing table with a different next hop address. This problem is resolved in Release 12.1(22)E3. (CSCed59370)
- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in Release 12.1(22)E3. (CSCed78149)
- Traffic might be lost when communication fails between the supervisor engine and the MSFC. This problem is resolved in Release 12.1(22)E3: an intentional reload occurs when communication fails between the supervisor engine and the MSFC. (CSCee39004)
- While traffic is flowing, CPU utilization might increase to a very high level if you reconfigure an EtherChannel from Layer 3 to Layer 2 and configure a Layer 3 VLAN interface for the EtherChannel. This problem is resolved in Release 12.1(22)E3. (CSCee41100)
- Traffic loss might occur on fabric-enabled modules when there are frequent OIRs. This problem is resolved in Release 12.1(22)E3. (CSCee44496, CSCee48403, CSCee78766)
- SNMP returns a null value for the SLB real server name. This problem is resolved in Release 12.1(22)E3. (CSCee60121)
- A memory leak might occur with Cisco IOS firewall authentication proxy configured. This problem is resolved in Release 12.1(22)E3. (CSCef14971)
- Occasionally, these modules might lose the ability to communicate over the Ethernet Out of Band Channel (EOBC) and reset:
  - WS-X6416-GBIC
  - WS-X6348-RJ-45
  - WS-X6148-RJ-45
  - WS-X6348-RJ-21

  - WS-X6148-RJ-21
  - WS-X6316-GE-TX
  - WS-X6324-100FX
  - WS-X6416-GE-MT
  - WS-X6024-10FL-MT

  This problem is resolved in Release 12.1(22)E3. (CSCef23843)

- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

  The Advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

  This problem is resolved in Release 12.1(22)E3. (CSCef46191)

- Traffic might be dropped if you enter the **no ip cef** global configuration command. This problem is resolved in Release 12.1(22)E3. (CSCin40371)
- A reload might occur when traffic enters a port configured with the **switchport protocol ip auto** command. This problem is resolved in Release 12.1(22)E3. (CSCin77984)

Resolved General Caveats in Release 12.1(22)E2

- The **no ip vrf** *vrf_name* command does not delete the VRF configuration. This problem is resolved in Release 12.1(22)E2. (CSCeb78347)
- PVLAN ports on an isolated VLAN on WS-6148-GE-TX and WS-6548-GE-TX switching modules might not be able to send or receive traffic through a promiscuous port.This problem is resolved in Release 12.1(22)E2. (CSCee45867)
- If the FIB TCAM is full, a memory leak or a reload might occur or you might observe high supervisor engine utilization. This problem is resolved in Release 12.1(22)E2. (CSCeb85827, CSCeb29888, CSCec14802, CSCec42634, CSCed58661, CSCee00311, CSCee22821)
- A reload might occur if you enter the **clear ip route *** command. This problem is resolved in Release 12.1(22)E2. (CSCee00311: refer to CSCeb85827)
- When you use local-proxy-arp and HSRP, the active MSFC could respond to ARP requests with the BIA MAC address and the redundant MSFC might keep cached ARP entries that should have been deleted. This problem is resolved in Release 12.1(22)E2. (CSCed72287)
- After you configure a tunnel to support DECnet with assigned DECnet cost and then delete the tunnel configuration, a reload might occur if you disable DECnet routing. This problem is resolved in Release 12.1(22)E2. (CSCed88563)
- Following switchover to a redundant supervisor engine, any EtherChannels on the newly active supervisor engine are not active and the newly redundant supervisor engine does not enter the standby state. This problem is resolved in Release 12.1(22)E2. (CSCee44248)

- OSPF area border routers (ABRs) might continue to generate summary link-state advertisements (LSAs) for obsolete nonbackbone intra-area routes. This problem is resolved in Release 12.1(22)E2. (CSCee36622)
- Traffic through a port-channel interface that has a Cisco IOS ACL configured might be dropped or switched in software after a reload or after switchover to a redundant supervisor engine or after you enter **shutdown** and **no shutdown** interface commands on a member port. This problem is resolved in Release 12.1(22)E2. (CSCee21772)
- A small (approximately 180 bytes) memory leak occurs when you delete a logical interface. This problem is resolved in Release 12.1(22)E2. (CSCee05413)
- If you change the STP root bridge, a Layer 2 loop might exist very briefly. This problem is resolved in Release 12.1(22)E2. (CSCed85411)

Resolved General Caveats in Release 12.1(22)E1

- OSM-1CHOC12/T1-SI T1 interfaces that have path coding violations (PCVs) might cause erroneous Layer 1 errors to be displayed for other T1 interfaces. This problem is resolved in Release 12.1(22)E1. (CSCed86486)
- Many memory allocation failure (MALLOCFAIL) messages might occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
  Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  This problem is resolved in Release 12.1(22)E1. (CSCdz32659)
- With certain configurations, a reload might occur when you enter the **show cdp entry * protocol** command. This problem is resolved in Release 12.1(22)E1. (CSCed40563)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in Release 12.1(22)E1. (CSCed93836, CSCdz84583)
- After Cisco IOS ACLs have been updated dynamically or after responding dynamically to an IDS signature, a reload might occur following attempts to access a low memory address. This problem is resolved in Release 12.1(22)E1. (CSCed35253)

- Receiving CDP packets with a host name that is 256 or more characters long might cause a memory leak in the CDP process. This problem is resolved in Release 12.1(22)E1. (CSCin67568)

Resolved General Caveats in Release 12.1(22)E

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

  This problem is resolved in Release 12.1(22)E. (CSCed65778)
- A reload might occur if one process is writing to NVRAM and another process is reading from NVRAM and the read fails. This problem is resolved in Release 12.1(22)E. (CSCec63011)
- In topologies with VLAN interfaces configured as intermediate multicast router connections, Protocol Independent Multicast (PIM) register and PIM register stop messages might loop between the intermediate routers until the TTL count expires. This problem is resolved in Release 12.1(22)E. (CSCed87886)
- A group of 8 ports on a WS-X6548-GE-TX switching module might stop forwarding traffic. This problem is resolved in Release 12.1(22)E. (CSCed68821)
- With server load balancing (SLB) configured on a Supervisor Engine 1 and an MSFC1, you might see INPUTQ messages and interfaces might stop passing traffic. This problem is resolved in Release 12.1(22)E. (CSCed49443)
- With high traffic levels and when the reverse forwarding path (RPF) towards the rendezvous point and the multicast source are different, partially hardware-switched multicast flows might not be forwarded correctly. This problem is resolved in Release 12.1(22)E. (CSCec80654)
- After "MALLOCFAIL" messages and tracebacks, a reload might occur. This problem is resolved in Release 12.1(22)E. (CSCec71297)
- With the **service compress-config** command or the **boot config** command in the configuration, a reload because of a bus error and stack overflow or stack corruption might occur if the configuration is larger than the NVRAM size and you enter the **show config** command simultaneously with the **write terminal** or **show running-config** command. This problem is resolved in Release 12.1(22)E. (CSCed45942)
- In releases where caveat CSCdz27200 is resolved, a reload might occur when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) flash card (for example, disk0). For example, this situation may occur when you enter the **show** *command_name* **| tee /append** *url* privileged EXEC command. This problem is resolved in Release 12.1(22)E. (CSCin57765)
- In releases where caveat CSCdz27200 is resolved, files copied to an ATA disk might be corrupt. This problem is resolved in Release 12.1(22)E. (CSCed44319)
- The DSCP value is incorrectly set to zero in NBAR traffic. This problem is resolved in Release 12.1(22)E. (CSCec49042)

- A reload might occur if you enter the **interface loopback** *interface_number* interface configuration command and the value of the *interface_number* argument is a 9-digit number that starts with 10. This problem is resolved in Release 12.1(22)E. (CSCec03907)
- Because the WCCP service group list is scanned in the order in which service groups are created, rather than by priority, with multiple dynamic WCCP services defined, traffic that matches the selection criteria for more than one service group is not redirected to the service group with the highest priority. This problem is resolved in Release 12.1(22)E. (CSCec55429)
- When Automatic Protection Switching (APS) is not configured on a POS interface, ignore an incrementing "COAPS" counter. This problem is resolved in Release 12.1(22)E. (CSCec89414)
- NetFlow Data Export (NDE) does not support multicast traffic, but NDE might export some multicast data. This problem is resolved in Release 12.1(22)E. (CSCec37069)
- With Web Cache Communication Protocol (WCCP) configured and the cache farm formed successfully, packet redirection to a cache might not occur. This problem is resolved in Release 12.1(22)E. (CSCuk47528)
- HSRP packets are sent with the IP TTL field set to 2 instead of 1. This does not affect HSRP operation because HSRP packets are sent to a Layer 2 multicast address. This problem is resolved in Release 12.1(22)E. (CSCuk31498)
- A reload might occur after you enter the **shutdown** and **no shutdown** interface configuration commands multiple times on different interfaces. This problem is resolved in Release 12.1(22)E. (CSCed55567)
- When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as "OID not increasing" might occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured but HSRP is not configured at all. This problem is resolved in Release 12.1(22)E. (CSCed52163)
- With Multiprotocol Label Switching (MPLS) configured, after accessing a freed Label Information Base (LIB) entry, this message might be displayed:

  ```
  %TIB-3-LCLTAG: 10.10.10.10/10.10.10.10, tag advert; unexpected tag state=13
  ```

  After the message is displayed, a reload might occur. This problem is resolved in Release 12.1(22)E. (CSCed47409)
- When configured as a PE router, if you change the layer encapsulation of a PPP, Frame Relay, or HDLC PE subinterface, ping traffic to a CE router might fail. This problem is resolved in Release 12.1(22)E. (CSCed13350)
- A switched virtual circuit (SVC) might not transition to the established state. This situation might cause ping failures. This problem is resolved in Release 12.1(22)E. (CSCec80061)
- With an ATA flash device, you might see this message:

  ```
  PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a different router or PC. A format
  in this router is required before an image can be booted from this device
  ```

  This problem is resolved in Release 12.1(22)E. (CSCec69091)
- You might see high CPU utilization if you enter the logging synchronous command for line con 0. This problem is resolved in Release 12.1(22)E. (CSCdy01705)
- When a Layer 3 VLAN interface is configured as an OSPF nonbroadcast network and a polling interval is configured for every OSPF neighbor, unnecessary ARPs are sent. This problem is resolved in Release 12.1(22)E. (CSCed26217)

- With Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) or IEEE 802.1s multiple spanning tree (MST) configured, when the root bridge in a spanning tree domain ages out, the remaining bridges reconverge after timing out the root bridge. During this reconvergence, a spanning tree loop might occur. This problem is resolved in Release 12.1(22)E. (CSCed00441)
- In releases where caveat CSCed00441 is resolved and with Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) or IEEE 802.1s, multiple spanning tree (MST) configured, when an edge port goes down, a topology change is generated. This problem is resolved in Release 12.1(22)E. (CSCed63897)
- Network Address Translation (NAT) does not work with WCCP configured. This problem is resolved in Release 12.1(22)E. (CSCeb28941)
- Occasionally, multicast traffic that should be completely Layer 3-switched is partially Layer 3-switched, which causes multicast packets to be dropped when the ACL TCAM is full. This problem is resolved in Release 12.1(22)E. (CSCin63402)
- With a Supervisor Engine 2, when a fabric-capable line card comes online and an RSPAN source session is configured, the RSPAN source session might stop working. When this happens, the traffic being monitored will not be replicated on the RSPAN VLAN. This problem is resolved in Release 12.1(22)E. (CSCin61989)
- The **show controller serial** command output is not complete. This problem is resolved in Release 12.1(22)E. (CSCin60835)
- With fall-back bridging configured, ARP fails after a switchover to the redundant supervisor engine. This problem is resolved in Release 12.1(22)E. (CSCed61632)
- When more than 12 VLOUs are used in a policy attached to an interface, the entries are expanded. If the expanded entries are for a non-deny ACE, the entries are not accurate. The resulting ACEs for the policy are also inaccurate. This problem is resolved in Release 12.1(22)E. (CSCed47753)
- A reload might occur when an exception is generated as the result of adding a policy. This problem is resolved in Release 12.1(22)E. (CSCed46684)
- Gigabit Ethernet negotiation does not work. This problem is resolved in Release 12.1(22)E. (CSCed19431)
- When a Border Gateway Protocol (BGP) process propagates routes that are learned from an interior Border Gateway Protocol (iBGP) peer to an external BGP (eBGP) peer, the eBGP peer should see these routes with the next-hop address of the originator's address, but the eBGP peer incorrectly sees the routes with the next-hop address of the router that propagates the routes instead of the router that originates the routes. This problem is resolved in Release 12.1(22)E. (CSCed15277)
- To avoid dropping into ROMMON, do not insert a WS-X6816-GBIC that does not have a DFC installed. This problem is resolved in Release 12.1(22)E. (CSCed14506)
- Malfunctioning PIM, MLSM, or mwheel processes might cause "CPUHOG" and "WATCHDOG" messages and reloads. This problem is resolved in Release 12.1(22)E. (CSCed12393)
- Weighted Fair Queuing WFQ over Frame Relay runs like first-in-first-out (FIFO). This problem is resolved in Release 12.1(22)E. (CSCed09383)
- A 512 MB small outline DIMM (SODIMM) registers as only 256 MB when you enter the **show diagnostic** command. This problem is resolved in Release 12.1(22)E. (CSCed07253)
- Occasionally, the nvram:/startup-config file cannot be read. This problem is resolved in Release 12.1(22)E. (CSCed06462)
- Layer 2 traffic might be dropped if policy-based routing (PBR) is enabled on a VLAN interface. This situation affects all traffic not permitted by the configured policy. This problem is resolved in Release 12.1(22)E. (CSCed05843)

- When the OSPF cost is changed on one of the upstream paths in the network and a request to delete or remove the stale entry is not received, the TTFIB table contains stale entries that causes traffic loss. This problem is resolved in Release 12.1(22)E. (CSCed01611)
- A FlexWAN module is not detected during the boot process causing it to be ignored during the startup configuration process. This problem is resolved in Release 12.1(22)E. (CSCed00781)
- Directly connected multicast enabled subnets might not be programmed correctly into the PFC. This problem is resolved in Release 12.1(22)E. (CSCed00394)
- Memory corruption causes the software to reload when an illegal write operation is performed by the authentication, authorization, and accounting (AAA) process. This problem is resolved in Release 12.1(22)E. (CSCec85347)
- Directed broadcasts to a destination network that is part of an MPLS VPN fail.This problem is resolved in Release 12.1(22)E. (CSCec75499)
- The **ip pim register source** command is not supported in Release 12.1E. This problem is resolved in Release 12.1(22)E. (CSCec70483)
- When protocol independent multicast (PIM) dense mode is enabled, an interface in the outgoing interface list may indicate it is in forwarding mode, but the P flag may be set to the group (S,G) state, which prevents the interface from forwarding packets. This problem is resolved in Release 12.1(22)E. (CSCec70428)
- L3-PS-DRVR messages are seen every 12 to 16 seconds. This problem is resolved in Release 12.1(22)E. (CSCec63833)
- When an interface that is configured with multiple IP multicast helper maps for the same group address and for different broadcast addresses is removed, it generates false memory-access errors. If the interface is reconfigured and removed again, the router will crash. This problem is resolved in Release 12.1(22)E. (CSCec63186)
- With a 13-slot chassis, a bus error and reload might occur if you configure EtherChannels that include any slot 13 ports. This problem is resolved in Release 12.1(22)E. (CSCec49438)
- Incorrect processing of received PIM packets causes IGMP snooping to fail. When this occurs, the system is unable to learn the correct outbound interface for the multicast traffic. This problem is resolved in Release 12.1(22)E. (CSCec46892)
- After you remove a Cisco IOS ACL from an interface, the packets continue to be passed or dropped as they would with the Cisco IOS ACL still attached. This problem is resolved in Release 12.1(22)E. (CSCec43666)
- With VLAN aging configured, the routed MAC (RM) bit might be set on the Layer 2 entries for routed traffic, which causes the entries to be purged every 5 minutes. One packet might be flooded and relearned for each purged entry. This problem is resolved in Release 12.1(22)E. (CSCec43605)
- A FIB-related memory leak might occur. This problem is resolved in Release 12.1(22)E. (CSCec43573)
- For BGP routes learned through a WAN interface, if the BGP neighbor goes down, the default route adjacency does not change if the default route learned through BGP had a better metric than a static route configured locally. This problem is resolved in Release 12.1(22)E. (CSCec41005)
- An IGMP packet flood might cause a reload. This problem is resolved in Release 12.1(22)E. (CSCec39132)
- With an MPLS PE configuration, some IP-to-tag adjacencies might be incorrectly installed on the switch processor after interfaces go up and down and a large number of BGP routes need to be resolved. This problem is resolved in Release 12.1(22)E. (CSCec30461)

- When Border Gateway Protocol (BGP) uses multihome interfaces to peer with the neighbors that are part of the same peer group or the same update group and you enter the neighbor next-hop-self router configuration command on routers of a peer group, the next-hop calculation is performed only on the first member of the peer group, and the same next-hop value is replicated to the rest of the peers instead of calculating the next hop based on the next-hop-self configuration. This problem is resolved in Release 12.1(22)E. (CSCec14415)
- When fragmenting MPLS traffic, a reload might occur after display of a "SYS-2-GETBUF" message. This problem is resolved in Release 12.1(22)E. (CSCeb16876)
- The PFC might not be programmed to provide Layer 3 switching for traffic that follows a static route to the null 0 interface. This problem is resolved in Release 12.1(22)E. (CSCea86396)
- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

  This problem is resolved in Release 12.1(22)E. (CSCea44227, CSCdx40184, CSCeb78836, CSCec76776, CSCed28873, CSCin56408)
- In releases where CSCdz75507 is resolved, you cannot configure fall-back bridging on any subinterface under a physical interface where MPLS is configured on another subinterface. This problem is resolved for ATM interfaces in Release 12.1(22)E. (CSCeb87433; also see resolved caveat CSCee00239)
- CBAC FTP-data sessions might stay in the "sis-closing" state because of out-of-order packet handling. This problem is resolved in Release 12.1(22)E. (CSCed03333)
- The Cisco IOS firewall authentication proxy feature might reject a connection. This problem is resolved in Release 12.1(22)E. (CSCea33481)
- Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

  This problem is resolved in Release 12.1(22)E. (CSCed68575)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the

sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

This problem is resolved in Release 12.1(22)E. (CSCed27956, CSCed38527)

- QoS access control list with Layer 4 port operation is not supported. This problem is resolved in Release 12.1(22)E. (CSCdx91720)
- A reload might occur if you apply an undefined crypto map to an interface. This problem is resolved in Release 12.1(22)E. (CSCin08118)
- A reload might occur if you establish an SSHv2 session immediately after the “Press RETURN to get started!” message appears on the console. This problem is resolved in Release 12.1(22)E. (CSCin48676)
- In a topology with overlapping networks, EIGRP might incorrectly remove a connected route if you add a new **network** command before you remove the old one. This problem is resolved in Release 12.1(22)E. (CSCed93804)
- With bursty multicast sources on the network, a reload might occur because of a watchdog timeout if a nondefault holdtime value is received in a Protocol Independent Multicast (PIM) join message. The holdtime value might be nondefault because it is from a non-Cisco network device or because the Internet Group Management Protocol (IGMP) query interval has been modified on an interface. This problem is resolved in Release 12.1(22)E. (CSCec70366)
- A reload might occur if you remove a **network** command from an interface where OSPF is configured and there is OSPF traffic from the interface in the OSPF queue. This problem is resolved in Release 12.1(22)E. (CSCec48816)
- When buffer allocation failures occur while free I/O memory is low, Protocol Independent Multicast (PIM) join messages might not be sent. This problem is resolved in Release 12.1(22)E. (CSCec40377)
- A reload because of memory corruption might occur when an IP Security (IPsec) generic routing encapsulation (GRE) tunnel carries multicast traffic. This problem is resolved in Release 12.1(22)E. (CSCec06341)
- If you enter the **ip verify unicast reverse-path** interface configuration command on ATM subinterfaces, some ingress traffic is dropped. This problem is resolved in Release 12.1(22)E. (CSCdt51547)
- In an SSM/IGMPv3 environment under a topology where a non-designated router (non-DR), but not the designated router (DR), is in the Shortest Path Tree (SPT), it may take the non-DR up to 3-1/2 minutes to prune and time-out its outgoing interface when all interested receivers have left an (s,g) group. This problem is resolved in Release 12.1(22)E. (CSCed12688)
- With a loopback cable from a trunk port connected to a WAN port acting as an MPLS/VPN interface, an unresolved default route causes the PFC to send packets to the MSFC for ARP resolution, which interferes with hardware switching of the packets exiting the loopback port. This problem is resolved in Release 12.1(22)E. (CSCed64844)

- TCP FIN and RST packets might be dropped, which causes a 3 to 4 second delay in retrieving web content, if a hardware-switched TCP connection carrying more than 1,000 packets per second is load balanced through IOS Firewall Load Balancing or Cisco IOS server load balancing. This problem is resolved in Release 12.1(22)E. (CSCed38956)
- With a PFC2 and with EtherChannels configured to include interfaces on different DFC-equipped switching modules, ARP traffic from a WS-X6066-SLB-APC Content Switching Module (CSM) that is running software version 3.2(2) and earlier might not be forwarded correctly. This problem is resolved in Release 12.1(22)E. (CSCed35745)
- A new vulnerability in the OpenSSL implementation for SSL has been announced on March 17, 2004.

  An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack. There are workarounds available to mitigate the effects of this vulnerability on Cisco products in the workaround section of this advisory. Cisco is providing fixed software, and recommends that customers upgrade to it when it is available.

  This advisory will be posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml

  This problem is resolved in Release 12.1(22)E. (CSCee00041)
- Following "cmd failed" messages for ATM configuration commands, an ATM interface might remain administratively down. This problem is resolved in Release 12.1(22)E. (CSCin40163)
- If the ACL specified in the **ip multicast boundary** *acl_name* **filter-autorp** command has non-wildcard entries, the filter-autorp functionality does not work. This problem is resolved in Release 12.1(22)E. (CSCed02952)
- When a real server is in a backup server farm, and static NAT is configured for that real server, IOS-SLB does not provide NAT for packets sourced by the real server. This problem is resolved in Release 12.1(22)E. (CSCec62611)
- The dynamic NAT pool allocation can reach 100% utilization if you configure a static NAT entry with an IP address that is part of a dynamic pool. This problem is resolved in Release 12.1(22)E. (CSCec54341)
- SSH packets are not marked with IP precedence 6. This problem is resolved in Release 12.1(22)E. (CSCeb73981)
- A reload might occur if you enter the **show frame-relay** command while another user is removing the **encapsulation frame-relay** interface configuration command while the show command is in the process of being displayed. This problem is resolved in Release 12.1(22)E. (CSCeb44256)
- With ISIS routing configured, an E3 or T3 port adapter might have its neighbors flap after a reload. This problem is resolved in Release 12.1(22)E. (CSCeb01905)
- Routing Information Protocol version 2 (RIPv2) routes get stuck in the routing table, even if the next hop interface is down. This problem is resolved in Release 12.1(22)E. (CSCea47597)
- Occasionally, characters that you enter over a virtual terminal connection are not echoed. This problem is resolved in Release 12.1(22)E. (CSCdz36877)
- Ping to the IP address of a local GRE tunnel interface fails. This problem is resolved in Release 12.1(22)E. (CSCdx74855)
- Occasionally when an IP EIGRP route changes disposition from internal to external and also increases in metric, a router receiving the updates might not update the routing table and leave the topology table entry with zero successors. This problem is resolved in Release 12.1(22)E. (CSCdw33164)

- A reload might occur when you enter the **shutdown** and **no shutdown** interface configuration command for the interface that connects to an IP EIGRP neighbor, and then you enter the **show ip eigrp neighbors** EXEC command. This problem is resolved in Release 12.1(22)E. (CSCdu59038)
- The BGP address family IPv4 **neighbor x.y.z.t peer-group** command appears twice in the configuration when entered only once. This problem is resolved in Release 12.1(22)E. (CSCdu18393)
- Address overloading might fail if you manually clear the NAT translation table. This problem is resolved in Release 12.1(22)E. (CSCdt95129)
- High-volume SNMP traffic might cause a reload. This problem is resolved in Release 12.1(22)E. (CSCed79519)
- DLSw might not work. This problem is resolved in Release 12.1(22)E. (CSCed40129)
- Traffic might flow in only one direction after assigning a LAN port to a different VLAN. This problem is resolved in Release 12.1(22)E. (CSCed20566)
- If you enter the **ip flow-export destination** command to configure multiple flow export destinations, you might observe high CPU utilization and dropped control packets, which can result in routing protocol timeouts and slow response during console access. This problem is resolved in Release 12.1(22)E. (CSCed15587)
- The WS-X6816-GBIC switching module might report a minor error after a reload and require an online insertion and removal (OIR) before it can be used. This problem is resolved in Release 12.1(22)E. (CSCed05332)
- Occasionally after a reload, the IDPROM is not read correctly on a WS-X6548-RJ-45 switching module that is equipped with a DFC, which holds the module in the “other” state. This problem is resolved in Release 12.1(22)E. (CSCed04988)
- An SNMP query to retrieve the policy maps attached to an interface that has multiple policy maps attached incorrectly aggregates the policy maps into a display showing only one policy map. This problem is resolved in Release 12.1(22)E. (CSCec72502)
- A Supervisor Engine 2 configured with the Cisco IOS-SLB RADIUS Load Balancing (RLB) feature might reload unexpectedly because of a bus error at an illegal address when you make changes to the Server Load Balancing (SLB) configuration. This problem is resolved in Release 12.1(22)E. (CSCec55377)
- The WS-X6548-RJ-21 module does not support the **mdix auto** command. This problem is resolved in Release 12.1(22)E. (CSCec50648)
- An IBC reset may cause the MSFC to drop packets. This problem is resolved in Release 12.1(22)E. (CSCec48379)
- Because a multicast router might fail to send a register stop message, the designated router sends register messages continuously. This problem is resolved in Release 12.1(22)E. (CSCec41693)
- With Multicast Source Discovery Protocol (MSDP) configured, a reload might occur if you enter the **show ip msdp peer** *ip_address* **advertised-SAs** command. This problem is resolved in Release 12.1(22)E. (CSCec23559)
- The MAC-move notification feature cannot be configured when there are EtherChannels formed from ports on different DFC-equipped modules. This problem is resolved in Release 12.1(22)E. (CSCec15149)
- VACLs do not work on routed RSPAN traffic. This problem is resolved in Release 12.1(22)E. (CSCeb61695)

- With a route in a different VPN routing and forwarding instance (VRF) attached to an interface, the interface might not be able to receive traffic being sent to an address that is configured on the MSFC. This problem is resolved in Release 12.1(22)E. (CSCeb52270)
- Following a reload with a large number of active interfaces, an Open Shortest Path First (OSPF) interface might be in the down state while the port and the line protocol might be in the up state, which causes missing OSPF neighbor adjacencies on the OSPF interface that is in the down state. This problem is resolved in Release 12.1(22)E. (CSCeb04048)
- With a complex Spanning Tree topology (for example, a high number of blocked ports in the same VLAN), if an inferior BPDU is received at approximately the same time that the message age timer expires, STP might send out BPDUs with obsolete information (for example, the previous root ID) for the duration of the maximum age timer, which can delay STP convergence. This problem is resolved in Release 12.1(22)E. (CSCea68988)
- With faulty hardware, continuous reloads might follow the display of an "SLCP Not Responding" message. This problem is resolved in Release 12.1(22)E. (CSCea57452)
- The **show interfaces** command output rate bits per second value is incorrect. This value is consistently high and does not correlate to actual traffic. This problem is resolved in Release 12.1(22)E. (CSCeb33104)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(22)E6, page 187
- Resolved FlexWAN Module Caveats in Release 12.1(22)E6, page 187
- Resolved FlexWAN Module Caveats in Release 12.1(22)E5, page 187
- Resolved FlexWAN Module Caveats in Release 12.1(22)E4, page 187
- Resolved FlexWAN Module Caveats in Release 12.1(22)E3, page 188
- Resolved FlexWAN Module Caveats in Release 12.1(22)E2, page 188
- Resolved FlexWAN Module Caveats in Release 12.1(22)E1, page 188
- Resolved FlexWAN Module Caveats in Release 12.1(22)E, page 188

Open FlexWAN Module Caveats in Release 12.1(22)E6

None.

Resolved FlexWAN Module Caveats in Release 12.1(22)E6

None.

Resolved FlexWAN Module Caveats in Release 12.1(22)E5

None.

Resolved FlexWAN Module Caveats in Release 12.1(22)E4

None.

Resolved FlexWAN Module Caveats in Release 12.1(22)E3

- Serial interfaces on a PA-MC-8TE1+ port adapter that are configured as part of a channel group continue to process packets when the interface is in the "admindown" state. The counters in the output of the **show interfaces serial** command might increment when the serial interface is shut down. This problem is resolved in Release 12.1(22)E3. (CSCin78325)

Resolved FlexWAN Module Caveats in Release 12.1(22)E2

- PA-A3-8T1IMA and PA-A3-8E1IMA port-adapter interfaces generate repeated "changed state to up" messages without corresponding "changed state to down" messages. This problem is resolved in Release 12.1(22)E2. (CSCin05262)
- EIGRP neighbors flap and output traffic is dropped when traffic on a PA-A3-8T1IMA or PA-A3-8E1IMA port-adapter interface is 40 percent or more of the non-real time variable bit rate (VBR-nrt) parameter. This problem is resolved in Release 12.1(22)E2. (CSCee50948)

Resolved FlexWAN Module Caveats in Release 12.1(22)E1

None.

Resolved FlexWAN Module Caveats in Release 12.1(22)E

- With a FlexWAN module, following a reload, you might see erroneous OIR-6-REMCARD messages and the FlexWAN module might reset. This problem is resolved for Frame Relay interfaces in Release 12.1(22)E. (CSCed53595)
- Operation, Administration, and Maintenance (OAM) permanent virtual circuits (PVCs) on PA-A3-8T1IMA or PA-A3-8E1IMA interfaces are not active after an OIR. This problem is resolved in Release 12.1(22)E. (CSCin65182)
- An administratively shut-down subinterface that is configured for Frame-Relay encapsulation might forward packets. This problem is resolved in Release 12.1(22)E. (CSCed78803)
- Following OIR of a PA-MC-8TE1+ port adapter, the output queue might be stuck. This problem is resolved in Release 12.1(22)E. (CSCec70301, CSCec70296)
- A service policy configured to allocate bandwidth to routing protocol control traffic on a fully utilized PA-MC-8TE1+ port adapter E1 link does not prevent the traffic from being dropped. This problem is resolved in Release 12.1(22)E. (CSCed36110)
- A 1-port E3 serial port adapter (PA-E3) might fail to recover to the "up/up" state even when the original cause of the failure is corrected. This problem is resolved in Release 12.1(22)E. (CSCec33028)
- The FlexWAN module may reload when it is booting up. This problem is resolved in Release 12.1(22)E. (CSCec55445)
- With heavy traffic through a PA-MC-T3 or PA-MC-E3 port adapter, a FlexWAN module might reload. This problem is resolved in Release 12.1(22)E. (CSCin62978)
- With a high traffic load, PA-A3-OC3, PA-A3-T3, and PA-A3-E3 port adapters might display an increasing "rx_no_buffer" counter in the output of the **show controllers atm** privileged EXEC command and some PVCs configured on the PA-A3 port adapter might stop receiving traffic. This problem is resolved in Release 12.1(22)E. (CSCin49458)
- The FlexWAN module might corrupt very small Frame Relay packets (for example, 2-byte X.25 SABM packets). This problem is resolved in Release 12.1(22)E. (CSCec59440)

- On a PA-A3 port adapter with distributed class-based weighted fair queuing (dCBWFQ) configured, when one bandwidth class is congested, there might be extra latency in another bandwidth class that is not congested. This problem is resolved in Release 12.1(22)E. (CSCeb61825)
- Output queue packet drops might occur on the priority queue of an E1 serial interface on a 1-port multichannel E3 port adapter (PA-MC-E3), after which the E1 serial interface becomes congested. This problem is resolved in Release 12.1(22)E. (CSCeb34203)

Service Module Caveats

- Open Service Module Caveats in Release 12.1(22)E6, page 189
- Resolved Service Module Caveats in Release 12.1(22)E6, page 189
- Resolved Service Module Caveats in Release 12.1(22)E5, page 189
- Resolved Service Module Caveats in Release 12.1(22)E4, page 189
- Resolved Service Module Caveats in Release 12.1(22)E3, page 189
- Resolved Service Module Caveats in Release 12.1(22)E2, page 189
- Resolved Service Module Caveats in Release 12.1(22)E1, page 189
- Resolved Service Module Caveats in Release 12.1(22)E, page 190

Open Service Module Caveats in Release 12.1(22)E6

None.

Resolved Service Module Caveats in Release 12.1(22)E6

None.

Resolved Service Module Caveats in Release 12.1(22)E5

None.

Resolved Service Module Caveats in Release 12.1(22)E4

None.

Resolved Service Module Caveats in Release 12.1(22)E3

- If a CSM server farm is configured with a real server name instead of a real server IP address, SNMP does not retrieve and display the IP address of the real server in the CISCO-SLB-MIB server table. This problem is resolved in Release 12.1(22)E3. (CSCed84042)

Resolved Service Module Caveats in Release 12.1(22)E2

None.

Resolved Service Module Caveats in Release 12.1(22)E1

None.

Resolved Service Module Caveats in Release 12.1(22)E

- If you add VLANs 1002-1005 to the allowed VLAN list for an SSL module, the SSL module might have a connectivity problem. This problem is resolved in Release 12.1(22)E. (CSCec60933)
- A traceback occurs if you enter the keepalive interface command on a tunnel with IPSEC on both sides. This problem is resolved in Release 12.1(22)E. (CSCec90162)
- BPDU packets are not sent to Firewall Services Module (FWSM) ports. When transparent-firewall mode is used, this situation may cause packet-forwarding loops when redundancy is enabled or when two Firewall Services Modules share the same VLANs. This problem is resolved in Release 12.1(22)E. (CSCec14054)

OSM Caveats

- Open OSM Caveats in Release 12.1(22)E6, page 190
- Resolved OSM Caveats in Release 12.1(22)E6, page 190
- Resolved OSM Caveats in Release 12.1(22)E5, page 190
- Resolved OSM Caveats in Release 12.1(22)E4, page 190
- Resolved OSM Caveats in Release 12.1(22)E3, page 190
- Resolved OSM Caveats in Release 12.1(22)E2, page 191
- Resolved OSM Caveats in Release 12.1(22)E1, page 191
- Resolved OSM Caveats in Release 12.1(22)E, page 191

Open OSM Caveats in Release 12.1(22)E6

None.

Resolved OSM Caveats in Release 12.1(22)E6

None.

Resolved OSM Caveats in Release 12.1(22)E5

None.

Resolved OSM Caveats in Release 12.1(22)E4

None.

Resolved OSM Caveats in Release 12.1(22)E3

- Multicast 127-byte UDP packets that egress from OSM-2OC12-POS interfaces have invalid checksums. This problem is resolved in Release 12.1(22)E3. (CSCec72798)
- Occasionally, OSM-2+4GE-WAN+ module interfaces do not pass traffic after a reload or OIR. This problem is resolved in Release 12.1(22)E3. (CSCed83227)
- The Gigabit Ethernet LAN ports on a OSM-2+4GE-WAN+ module might be reported as administratively “up/up” when there is a GBIC installed but no cable attached. This problem is resolved in Release 12.1(22)E3. (CSCee01868)

- The interfaces on an OSM-2+4GE-WAN+ module might be reported as administratively "up/up" when there is no GBIC installed. This problem is resolved in Release 12.1(22)E3. (CSCee35867)
- If you have an input service policy that is configured only to police attached to an OSM interface and you do not have an output service policy attached to the OSM interface and you OIR another module, the OSM might reset. This problem is resolved in Release 12.1(22)E3. (CSCee42074)
- Traffic loss might occur on OSMs when there are frequent OIRs. This problem is resolved in Release 12.1(22)E3. (CSCee54642)
- OSM ATM interfaces do not support the SNMP lowerLayerDown value defined in RFC 2863. This problem is resolved in Release 12.1(22)E3. (CSCee56269)

Resolved OSM Caveats in Release 12.1(22)E2

- An OSM-12CT3/T1 module with an E1 channel group configured is powered down. This problem is resolved in Release 12.1(22)E2. (CSCee42278)
- An OSM might be reset following an online insertion and removal (OIR) of a Switch Fabric Module (SFM) or during periods of heavy traffic. This problem is resolved in Release 12.1(22)E2. (CSCin37112)
- A reload might occur if you enter a **show controllers sonet** command with an invalid number for a T1 interface on a OSM-1CHOC12/T1-SI or OSM-12CT3/T1 module. This problem is resolved in Release 12.1(22)E2. (CSCee50911)
- OSM-1CHOC12 modules become unresponsive and are power cycled. This problem is resolved in Release 12.1(22)E2. (CSCee45508)

Resolved OSM Caveats in Release 12.1(22)E1

None.

Resolved OSM Caveats in Release 12.1(22)E

- The serial interface input and output counters for an OSM always show 0 when you enter the **show interfaces serial** command. This problem is resolved in Release 12.1(22)E. (CSCed07367)
- An E3 serial interface on an OSM-1CHOC12/T3-SI module might be inactive after you enter **shutdown** and **no shutdown** commands. This problem is resolved in Release 12.1(22)E. (CSCed92724)
- OSM-4GE-WAN interfaces remain in the "up/up" state when the other end of the link is inactive. This problem is resolved in Release 12.1(22)E. (CSCec79460)
- If you delete and recreate Frame Relay subinterfaces in random order on OSM POS interfaces, some traffic might be sent to the wrong subinterface. This problem is resolved in Release 12.1(22)E. (CSCec67501)
- When EoMPLS virtual circuits (VCs) are loadbalanced across an OSM-2+4GE-WAN+ physical interface and a subinterface, the OSM reloads if you remove a service policy from the physical interface. This problem is resolved in Release 12.1(22)E. (CSCec65147)
- VRF ping packets are counted by the input counters for OSM physical interfaces, but not by the subinterface input counters. This problem is resolved in Release 12.1(22)E. (CSCea74537)
- OSM MLPPP interfaces do not support payload IPv4 protocol id compression in hardware. This problem is resolved in Release 12.1(22)E. (CSCed76259)
- An OC-12 POS OSM might reset as a result of memory corruption. This problem is resolved in Release 12.1(22)E. (CSCec59550)

- Distributed CEF switching does not work for multilink interface egress traffic. This problem is resolved in Release 12.1(22)E. (CSCec55650)
- The 64-bit counter on the OSM-2+4GE-WAN+ main interface shows an incorrect value of zero. This problem is resolved in Release 12.1(22)E. (CSCec34010)
- With CRC32 configured on OSM interfaces, priority queues have high latency with line-rate traffic. This problem is resolved in Release 12.1(22)E. (CSCec62800)
- On OC-12c OSMs, the **show controller pos** *interface* **pm** command displays incorrect optics information. This problem is resolved in Release 12.1(22)E. (CSCec48974)
- On OSM-2+4GE-WAN+ modules, the **ip mtu** interface command incorrectly cannot increase the MTU from the size set with the **mtu** interface command. This problem is resolved in Release 12.1(22)E. (CSCec03984)
- Parallel Express Forwarding (PXF) CEF load balancing does not work. This problem is resolved in Release 12.1(22)E. (CSCdu47678)

Release 12.1(20)E and Rebuilds

- General Caveats, page 192
- FlexWAN Caveats, page 207
- Service Module Caveats, page 209
- OSM Caveats, page 210

General Caveats

- Open General Caveats in Release 12.1(20)E6, page 192
- Resolved General Caveats in Release 12.1(20)E6, page 192
- Resolved General Caveats in Release 12.1(20)E3, page 194
- Resolved General Caveats in Release 12.1(20)E2, page 196
- Resolved General Caveats in Release 12.1(20)E, page 200

Open General Caveats in Release 12.1(20)E6

None.

Resolved General Caveats in Release 12.1(20)E6

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.

2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

This problem is resolved in Release 12.1(20)E6. (CSCed78149, CSCef44225, CSCef44699, CSCef60659, CSCsa59600)

- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

  The Advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

  This problem is resolved in Release 12.1(20)E6. (CSCef46191)

- OSPF area border routers (ABRs) might continue to generate summary link-state advertisements (LSAs) for obsolete nonbackbone intra-area routes. This problem is resolved in Release 12.1(20)E6. (CSCee36622)
- When an OSPF external route has a forwarding address with a next hop address in the routing table, the next hop address does not get updated in the type 5 link-state advertisement (LSA) when the forwarding address gets a more specific entry in the routing table with a different next hop address. This problem is resolved in Release 12.1(20)E6. (CSCed59370)
- Ping to the IP address of a local GRE tunnel interface fails. This problem is resolved in Release 12.1(20)E6. (CSCdx74855)
- Traffic through a port-channel interface that has a Cisco IOS ACL configured might be dropped or switched in software after a reload or after switchover to a redundant supervisor engine or after you enter **shutdown** and **no shutdown** interface commands on a member port. This problem is resolved in Release 12.1(20)E6. (CSCee21772)
- SNMP traps are sent for every Internet Key Exchange (IKE) timeout and rekey but not for every IPsec timeout and rekey. This situation might generate many false alerts that an IKE tunnel is down when the IKE tunnel is torn down but immediately rebuilt. Releases where CSCee91044 is resolved do not send SNMP traps that are sent for normal IKE operation. This problem is resolved in Release 12.1(20)E6. (CSCee91044)

Resolved General Caveats in Release 12.1(20)E3

- Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

  This problem is resolved in Release 12.1(20)E3. (CSCed65778)
- Address overloading might fail if you manually clear the NAT translation table. This problem is resolved in Release 12.1(20)E3. (CSCdt95129)
- With certain configurations, a reload might occur when you enter the **show cdp entry * protocol** command. This problem is resolved in Release 12.1(20)E3. (CSCed40563)
- Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

  This problem is resolved in Release 12.1(20)E3. (CSCed68575)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in Release 12.1(20)E3. (CSCed93836, CSCdz84583)

- With a route in a different VPN routing and forwarding instance (VRF) attached to an interface, the interface might not be able to receive traffic being sent to an address that is configured on the MSFC. This problem is resolved in Release 12.1(20)E3. (CSCeb52270)
- A reload might occur if you apply an undefined crypto map to an interface. This problem is resolved in Release 12.1(20)E3. (CSCin08118)
- Traffic might be dropped if you enter the **no ip cef** global configuration command. This problem is resolved in Release 12.1(20)E3. (CSCin40371)
- With MD5 password encryption configured, the software does not correctly verify that all configured TCP options can be sent in a TCP packet, which can cause this message to be displayed:

  ```
  %TCP-6-TOOBIG: Tty0, too many bytes of options (44)
  ```

  This problem is resolved in Release 12.1(20)E3. (CSCeb07106)
- A reload might occur if you establish an SSHv2 session immediately after the "Press RETURN to get started!" message appears on the console. This problem is resolved in Release 12.1(20)E3. (CSCin48676)
- In a topology with overlapping networks, EIGRP might incorrectly remove a connected route if you add a new **network** command before you remove the old one. This problem is resolved in Release 12.1(20)E3. (CSCed93804)
- When you configure BGP peergroups, spurious memory access messages are displayed. This problem is resolved in Release 12.1(20)E3. (CSCec78347)
- With bursty multicast sources on the network, a reload might occur because of a watchdog timeout if a nondefault holdtime value is received in a Protocol Independent Multicast (PIM) join message. The holdtime value might be nondefault because it is from a non-Cisco network device or because the Internet Group Management Protocol (IGMP) query interval has been modified on an interface. This problem is resolved in Release 12.1(20)E3. (CSCec70366)
- A reload might occur if you remove a **network** command from an interface where OSPF is configured and there is OSPF traffic from the interface in the OSPF queue. This problem is resolved in Release 12.1(20)E3. (CSCec48816)
- When buffer allocation failures occur while free I/O memory is low, Protocol Independent Multicast (PIM) join messages might not be sent. This problem is resolved in Release 12.1(20)E3. (CSCec40377)
- A reload because of memory corruption might occur when an IP Security (IPsec) generic routing encapsulation (GRE) tunnel carries multicast traffic. This problem is resolved in Release 12.1(20)E3. (CSCec06341)
- Receiving CDP packets with a host name that is 256 or more characters long might cause a memory leak in the CDP process. This problem is resolved in Release 12.1(20)E3. (CSCin67568)
- Following "cmd failed" messages for ATM configuration commands, an ATM interface might remain administratively down. This problem is resolved in Release 12.1(20)E3. (CSCin40163)

- A new vulnerability in the OpenSSL implementation for SSL has been announced on March 17, 2004.

  An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack. There are workarounds available to mitigate the effects of this vulnerability on Cisco products in the workaround section of this advisory. Cisco is providing fixed software, and recommends that customers upgrade to it when it is available.

  This advisory will be posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml

  This problem is resolved in Release 12.1(20)E3. (CSCee00041)
- After Cisco IOS ACLs have been updated dynamically or after responding dynamically to an IDS signature, a reload might occur following attempts to access a low memory address. This problem is resolved in Release 12.1(20)E3. (CSCed35253)
- The dynamic NAT pool allocation can reach 100% utilization if you configure a static NAT entry with an IP address that is part of a dynamic pool. This problem is resolved in Release 12.1(20)E3. (CSCec54341)
- Following a reload with a large number of active interfaces, an Open Shortest Path First (OSPF) interface might be in the down state while the port and the line protocol might be in the up state, which causes missing OSPF neighbor adjacencies on the OSPF interface that is in the down state. This problem is resolved in Release 12.1(20)E3. (CSCeb04048)
- If you enter the **ip verify unicast reverse-path** interface configuration command on ATM subinterfaces, some ingress traffic is dropped. This problem is resolved in Release 12.1(20)E3. (CSCdt51547)
- Many memory allocation failure (MALLOCFAIL) messages might occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
  Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  This problem is resolved in Release 12.1(20)E3. (CSCdz32659)
- With both static and dynamic Port Address Translation (PAT) configured and if the **ip nat pool** *inside_pool_name* command has been entered for only one IP address, the IP addresses that are used for overloading might be used as one-to-one translations. This problem is resolved in Release 12.1(20)E3. (CSCdx19396)

Resolved General Caveats in Release 12.1(20)E2

- With server load balancing (SLB) configured on a Supervisor Engine 1 and an MSFC1, you might see INPUTQ messages and interfaces might stop passing traffic. This problem is resolved in Release 12.1(20)E2. (CSCed49443)
- With high traffic levels and when the reverse forwarding path (RPF) towards the rendezvous point and the multicast source are different, partially hardware-switched multicast flows might not be forwarded correctly. This problem is resolved in Release 12.1(20)E2. (CSCec80654)
- After “MALLOCFAIL” messages and tracebacks, a reload might occur. This problem is resolved in Release 12.1(20)E2. (CSCec71297)

- With Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) or IEEE 802.1s multiple spanning tree (MST) configured, when the root bridge in a spanning tree domain ages out, the remaining bridges reconverge after timing out the root bridge. During this reconvergence, a spanning tree loop might occur. This problem is resolved in Release 12.1(20)E2. (CSCed00441)
- The PFC might not be programmed to provide Layer 3 switching for traffic that follows a static route to the null 0 interface. This problem is resolved in Release 12.1(20)E2. (CSCea86396)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in Release 12.1(20)E2. (CSCed27956, CSCed38527)
- In releases where caveat CSCdz27200 is resolved, a reload might occur when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) flash card (for example, disk0). For example, this situation may occur when you enter the **show** *command_name* **| tee /append** *url* privileged EXEC command. This problem is resolved in Release 12.1(20)E2. (CSCin57765)
- When a Border Gateway Protocol (BGP) process propagates routes that are learned from an interior Border Gateway Protocol (iBGP) peer to an external BGP (eBGP) peer, the eBGP peer should see these routes with the next-hop address of the originator's address, but the eBGP peer incorrectly sees the routes with the next-hop address of the router that propagates the routes instead of the router that originates the routes. This problem is resolved in Release 12.1(20)E2. (CSCed15277)
- To avoid dropping into ROMMON, do not insert a WS-X6816-GBIC that does not have a DFC installed. This problem is resolved in Release 12.1(20)E2. (CSCed14506)
- Occasionally, the nvram:/startup-config file cannot be read. This problem is resolved in Release 12.1(20)E2. (CSCed06462)
- Directly connected multicast enabled subnets might not be programmed correctly into the PFC. This problem is resolved in Release 12.1(20)E2. (CSCed00394)
- L3-PS-DRVR messages are seen every 12 to 16 seconds. This problem is resolved in Release 12.1(20)E2. (CSCec63833)
- With VLAN aging configured, the routed MAC (RM) bit might be set on the Layer 2 entries for routed traffic, which causes the entries to be purged every 5 minutes. One packet might be flooded and relearned for each purged entry. This problem is resolved in Release 12.1(20)E2. (CSCec43605)

- A FIB-related memory leak might occur. This problem is resolved in Release 12.1(20)E2. (CSCec43573)
- For BGP routes learned through a WAN interface, if the BGP neighbor goes down, the default route adjacency does not change if the default route learned through BGP had a better metric than a static route configured locally. This problem is resolved in Release 12.1(20)E2. (CSCec41005)
- An IGMP packet flood might cause a reload. This problem is resolved in Release 12.1(20)E2. (CSCec39132)
- When Border Gateway Protocol (BGP) uses multihome interfaces to peer with the neighbors that are part of the same peer group or the same update group and you enter the neighbor next-hop-self router configuration command on routers of a peer group, the next-hop calculation is performed only on the first member of the peer group, and the same next-hop value is replicated to the rest of the peers instead of calculating the next hop based on the next-hop-self configuration. This problem is resolved in Release 12.1(20)E2. (CSCec14415)
- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

  This problem is resolved in Release 12.1(20)E2. (CSCdx40184, CSCdx76632, CSCea46342, CSCeb78836, CSCec76776, CSCed28873, CSCin56408)
- When fragmenting MPLS traffic, a reload might occur after display of a “SYS-2-GETBUF” message. This problem is resolved in Release 12.1(20)E2. (CSCeb16876)
- With a complex Spanning Tree topology (for example, a high number of blocked ports in the same VLAN), if an inferior BPDU is received at approximately the same time that the message age timer expires, STP might send out BPDUs with obsolete information (for example, the previous root ID) for the duration of the maximum age timer, which can delay STP convergence. This problem is resolved in Release 12.1(20)E2. (CSCea68988)
- When an interface that is configured with multiple IP multicast helper maps for the same group address and for different broadcast addresses is removed, it generates false memory-access errors. If the interface is reconfigured and removed again, the router will crash. This problem is resolved in Release 12.1(20)E2. (CSCec63186)
- When protocol independent multicast (PIM) dense mode is enabled, an interface in the outgoing interface list may indicate it is in forwarding mode, but the P flag may be set to the group (S,G) state, which prevents the interface from forwarding packets. This problem is resolved in Release 12.1(20)E2. (CSCec70428)
- The **ip pim register source** command is not supported in Release 12.1E. This problem is resolved in Release 12.1(20)E2. (CSCec70483)
- Memory corruption causes the software to reload when an illegal write operation is performed by the authentication, authorization, and accounting (AAA) process. This problem is resolved in Release 12.1(20)E2. (CSCec85347)
- The **show controller serial** command output is not complete. This problem is resolved in Release 12.1(20)E2. (CSCin60835)

- SSH Version 1 does not work. This problem is resolved in Release 12.1(20)E2. (CSCed47810)
- When the OSPF cost is changed on one of the upstream paths in the network and a request to delete or remove the stale entry is not received, the TTFIB table contains stale entries that causes traffic loss. This problem is resolved in Release 12.1(20)E2. (CSCed01611)
- A Catalyst 6500 switch with an MSFC
- Layer 2 traffic might be dropped if policy-based routing (PBR) is enabled on a VLAN interface. This situation affects all traffic not permitted by the configured policy. This problem is resolved in Release 12.1(20)E2. (CSCed05843)
- A Catalyst 6500 switch with an MSFC may drop Layer 2 traffic if policy-based routing is enabled on the VLAN interface of the MSFC. This situation will affect all traffic not permitted by the configured policy. This problem is resolved in Release 12.1(20)E2. (CSCed05843)
- A 512 MB small outline DIMM (SODIMM) registers as only 256 MB when you enter the **show diagnostic** command. This problem is resolved in Release 12.1(20)E2. (CSCed07253)
- Weighted Fair Queuing WFQ over Frame Relay runs like first-in-first-out (FIFO). This problem is resolved in Release 12.1(20)E2. (CSCed09383)
- Malfunctioning PIM, MLSM, or mwheel processes might cause “CPUHOG” and “WATCHDOG” messages and reloads. This problem is resolved in Release 12.1(20)E2. (CSCed12393)
- Gigabit Ethernet negotiation does not work. This problem is resolved in Release 12.1(20)E2. (CSCed19431)
- On the WS-6548-GE-TX and WS-6148-GE-TX modules, the functionality for the **mls qos trust ip-precedence** and **mls qos trust dscp** commands is reversed. This problem is resolved in Release 12.1(20)E2. (CSCed38413)
- A Catalyst 6500 series switch crashes when an exception is generated as the result of adding a policy. This problem is resolved in Release 12.1(20)E2. (CSCed46684)
- A reload might occur when an exception is generated as the result of adding a policy. This problem is resolved in Release 12.1(20)E2. (CSCed46684)
- When more than 12 VLOUs are used in a policy attached to an interface, the entries are expanded. If the expanded entries are for a non-deny ACE, the entries are not accurate. The resulting ACEs for the policy are also inaccurate. This problem is resolved in Release 12.1(20)E2. (CSCed47753)
- With a Supervisor Engine 2, when a fabric-capable line card comes online and an RSPAN source session is configured, the RSPAN source session might stop working. When this happens, the traffic being monitored will not be replicated on the RSPAN VLAN. This problem is resolved in Release 12.1(20)E2. (CSCin61989)
- Occasionally, multicast traffic that should be completely Layer 3-switched is partially Layer 3-switched, which causes multicast packets to be dropped when the ACL TCAM is full. This problem is resolved in Release 12.1(20)E2. (CSCin63402)
- QoS access control list with Layer 4 port operation is not supported. This problem is resolved in Release 12.1(20)E2. (CSCdx91720)
- The output rate bits per second value is incorrect. This value is consistently high and does not correlate to actual traffic. This problem is resolved in Release 12.1(20)E2. (CSCeb33104)
- With an MPLS PE configuration, some IP-to-tag adjacencies might be incorrectly installed on the switch processor after interfaces go up and down and a large number of BGP routes need to be resolved. This problem is resolved in Release 12.1(20)E2. (CSCec30461)

- After you remove a Cisco IOS ACL from an interface, the packets continue to be passed or dropped as they would with the Cisco IOS ACL still attached. This problem is resolved in Release 12.1(20)E2. (CSCec43666)
- Incorrect processing of received PIM packets causes IGMP snooping to fail. When this occurs, the system is unable to learn the correct outbound interface for the multicast traffic. This problem is resolved in Release 12.1(20)E2. (CSCec46892)
- With a 13-slot chassis, a bus error and reload might occur if you configure EtherChannels that include any slot 13 ports. This problem is resolved in Release 12.1(20)E2. (CSCec49438)

Resolved General Caveats in Release 12.1(20)E

- Incorrect traffic loss occurs if you enter a **shutdown** command and then a **no shutdown** command on a Layer 3 VLAN interface that has HSRP configured. This problem is resolved in Release 12.1(20)E. (CSCec26522)
- With port security enabled, a memory leak might occur. This problem is resolved in Release 12.1(20)E. (CSCec14266)
- A redundant supervisor engine might incorrectly run out of memory while in the standby state and be unable to support a switchover. This problem is resolved in Release 12.1(20)E. (CSCec08966)
- After an RPR+ switchover, if you have configured the **mls ip directed broadcast** command, all broadcast traffic is sent to the MSFC to be processed in software. This problem is resolved in Release 12.1(20)E. (CSCec07319)
- Following a reload, a Supervisor Engine 2 with the **no mls qos channel-consistency** command configured might display an erroneous “qos-card type” mismatch message for an EtherChannel and incorrectly refuse to include some of the ports in the EtherChannel. This problem is resolved in Release 12.1(20)E. (CSCec00966)
- With CBAC and RPR+ redundancy configured, all TCP and UPD sessions fail after a switchover to the redundant supervisor engine. This problem is resolved in Release 12.1(20)E. (CSCeb87003)
- Some traffic that ingresses through one DFC-equipped module and egresses through another DFC-equipped module might be dropped. This problem is resolved in Release 12.1(20)E. (CSCeb83650)
- Multicast traffic that should be Layer 3 switched in hardware might be dropped or routed in software on the MSFC. This problem is resolved in Release 12.1(20)E. (CSCeb80373)
- With PBR configured on an interface, if the link goes down or if you enter a clear arp command, traffic that should be Layer 3 switched in hardware might be routed in software on the MSFC. This problem is resolved in Release 12.1(20)E. (CSCeb78050)
- The **scheduler allocate command** process-time default value is too small (200 microseconds, changed to 800 microseconds with this fix). The **no scheduler allocate** command does not return the configuration to default values. These problems are resolved in Release 12.1(20)E. (CSCeb75803)
- If you configure the **mac-address-table aging-time** command with a nonzero value, a static MAC address for traffic that egresses through a DFC-equipped card might change to a dynamic MAC address. This problem is resolved in Release 12.1(20)E. (CSCeb72014)
- With an IP multicast router directly connected to both a source and a receiver, and when the shortest path tree (SPT) threshold is configured as infinite, (S,G) entries are deleted every minute, which may cause packet loss about once per minute. This problem is resolved in Release 12.1(20)E. (CSCeb30338)

- A reload might occur when you enter a **show** command that is related to IP multicast if the "more" prompt has been displayed for a long period of time. This problem is resolved in Release 12.1(20)E. (CSCea81029)
- Cisco products running Cisco IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and Cisco IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

  This problem is resolved in Release 12.1(20)E. (CSCea32240)
- With other fabric-enabled modules installed, a WS-X6816-GBIC module does not come online after a hot insert or software reset. This problem is resolved in Release 12.1(20)E. (CSCec27072)
- A reload might occur if you delete a VPN routing and forwarding (VRF) instance while the **show ip vrf** *vrf_name* EXEC command executes. This problem is resolved in Release 12.1(20)E. (CSCea83675)
- New vulnerabilities in the OpenSSL implementation for SSL have been announced.

  An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device is vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml

  This problem is resolved in Release 12.1(20)E. (CSCec46274)
- With the Response Time Reporter (RTR) feature configured, spurious accesses might occur. This problem is resolved in Release 12.1(20)E. (CSCdy56859)
- A port in the STP loop guard loop-inconsistent state sends BPDUs and if is elected as the designated port on the segment, it does not recover from the loop-inconsistent state. This problem is resolved in Release 12.1(20)E. (CSCeb06811)
- An OSPF designated router does not generate a network link-state advertisement (LSA) for a broadcast network when another interface on the designated router has an administratively shut down interface with a duplicate address configured with the OSPF passive-interface command. This problem is resolved in Release 12.1(20)E. (CSCea35186)
- With Internet Group Management Protocol (IGMP) and IP Protocol Independent Multicast (PIM) enabled, continual tracebacks might occur when you perform an online insertion and removal (OIR) of a module. This problem is resolved in Release 12.1(20)E. (CSCec13278)
- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

This problem is resolved in Release 12.1(20)E. (CSCdu53656)

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.1(20)E. (CSCea28131)

- When operating in truncated mode following an SFM reset, traffic might not pass through ports on a WS-X6516-GBIC switching module because there might be no learned MAC entries in the MAC address table for the traffic. This problem is resolved in Release 12.1(20)E. (CSCea87650)
- With ARP enabled on ATM interfaces, you might see this message:

  ```
  %ALIGN-3-CORRECT: Alignment correction made
  ```

  This problem is resolved in Release 12.1(20)E. (CSCea80820)

- It is possible for an invalid **override-mac-address** command to be accepted at boot time if you use a configuration file from one system on another. This problem is resolved in Release 12.1(20)E. (CSCeb83558)
- The **squeeze** command might cause high CPU utilization for several minutes. This problem is resolved in Release 12.1(20)E. (CSCdz60750)
- A reload might follow receipt of a corrupt CPD packet. This problem is resolved in Release 12.1(20)E. (CSCec25430)
- With data-link switching (DLSw) configured, Ethernet Redundancy (ER) might not work on Inter-Switch Link (ISL) trunks. This problem is resolved in Release 12.1(20)E. (CSCec10234)
- Occasionally a bus error and reload might occur if an MPLS packet triggers the sending of an Internet Control Message Protocol (ICMP) packet. This problem is resolved in Release 12.1(20)E. (CSCeb27452)
- The WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX switching modules do not support ingress SPAN sources when the switch is operating in truncated mode or in compact mode. This problem is resolved in Release 12.1(20)E. (CSCeb08796)
- The default Operation Administration and Maintenance (OAM) intercept configuration drops OAM F5 END loopback cells. This problem is resolved in Release 12.1(20)E. (CSCdw41639)
- Service Assurance Agent (SAA) 2.1.1 returns the following message:

  ```
  Latest Oper Sense: httpError for HTTP status code 200.
  ```

  This problem is resolved in Release 12.1(20)E. (CSCeb64604)

- The configuration file repeatedly adds the same ACL remark, which makes the configuration file size very large. This problem is resolved in Release 12.1(20)E. (CSCdy36082)
- Approximately one second of frame loss occurs when a previously disconnected member of a PAGP-managed GEC is reconnected. This problem is resolved in Release 12.1(20)E. (CSCdz58247)
- If there are any open VTY lines when a RPR+ switchover occurs, these lines are displayed as “idle” or “never” with no location indicated after the switchover. These lines cannot be cleared using the **clear line** command. This problem is resolved in Release 12.1(20)E. (CSCea17268)
- When configuring RIPv2 on a router, spurious memory access may occur and tracebacks may be generated. This problem is resolved in Release 12.1(20)E. (CSCea22843)

- Sessions to linecards will fail if you enter the **ip telnet source-interface** command and the specified interface is an up/up state. This problem is resolved in Release 12.1(20)E. (CSCea36425)
- Layer 2 and Layer 3 switched counters remain at 0 after you enter the **show interface vlan** command. This problem is resolved in Release 12.1(20)E. (CSCea69116)
- The **stack-mib portname** command for switchport-configured physical interfaces gets erased from the startup configuration after a reboot. This problem is resolved in Release 12.1(20)E. (CSCea83414)
- NetFlow v5 cannot be exported from a Catalyst 7600 series router through the POS interface. NDE sends ARP requests for the NetFlow export destination. This problem is resolved in Release 12.1(20)E. (CSCea83603)
- A Catalyst 6500 series switch cannot reliably ping the Gigabit Ethernet interface of another directly connected Catalyst 6500 series switch when the same access list is applied to both the Gigabit Ethernet and ATM FlexWAN interfaces. This problem is resolved in Release 12.1(20)E. (CSCea86443)
- When you disconnect the cable between a WS-X6348-RJ-21V module and an IBM FE Open Systems Adapter Express (OSA/E), and then reconnect the cable, the link does not come back up. This problem is resolved in Release 12.1(20)E. (CSCea90470)
- A global command is needed for enabling link state messages on interfaces. This problem is resolved in Release 12.1(20)E. (CSCeb06765)
- When Cisco IOS Server Load Balancing (SLB) is configured, the following message may be generated when a Response Time Reporter (RTR) HTTP probe runs:

  ```
  IDMGR-3-INVALID_ID: bad id in id_to_ptr
  ```

  This problem is resolved in Release 12.1(20)E. (CSCeb19074)
- The ENTITY-MIB entPhysicalIsFRU displays “false” (2) for all field replaceable units. This problem is resolved in Release 12.1(20)E. (CSCeb21058)
- If the TCAM is full and the entries are being switched by software, a Catalyst 6500 series switch or Cisco 7600 series router may reload and display the following error message:

  ```
  %SYS-SP-2-WATCHDOG: Process aborted on watchdog timeout, process = FIB Control Task
  ```

  This problem is resolved in Release 12.1(20)E. (CSCeb36253)
- On a system with redundant Supervisor Engines running Cisco IOS Release 12.1(19)E that is functioning as an external router to a Cisco 5000 series switch, FCP messages similar to this may be displayed:

  ```
  FCP: shortcut ack msg for different router XXXX.XXXX.XXXX
  ```

  These messages are informational only. This problem is resolved in Release 12.1(20)E. (CSCeb44823)
- The system resets when the AAA protocol is configured for accounting. This problem is resolved in Release 12.1(20)E. (CSCeb42177)
- The following message might be followed by a reload:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0xX, ra=0xXXXXXXXX, sp=0xXXXXXXXX
  ```

  This problem is resolved in Release 12.1(20)E. (CSCeb48670)
- When you enter the **show policy-map interface** [**interface**] command on a system with a Supervisor Engine 2 and MSFC2, a system reload may occur. This problem is resolved in Release 12.1(20)E. (CSCeb49634)

- When there is insufficient memory, crash information is not generated after a Supervisor Engine reload. This problem is resolved in Release 12.1(20)E. (CSCeb51785)
- Cisco 7603 switches running Cisco IOS Release 12.1(19)E and using 950 Watt DC power supplies might keep modules in a power-deny state. This problem is resolved in Release 12.1(20)E. (CSCeb57796)
- Ethernet interface counters are updated only at 10-second intervals, instead of in real-time and on-demand. This problem is resolved in Release 12.1(20)E. (CSCec02790)
- An autonomous system border router (ASBR) might not update the forwarding address in self-generated LSAs if the interface with the forwarding address was removed from the OSPF domain. This problem is resolved in Release 12.1(20)E. (CSCdt45079)
- A Cisco 7200 series router may experience a memory leak caused by the Border Gateway Protocol (BGP) I/O process. This problem is resolved in Release 12.1(20)E. (CSCdu43164)
- Non-facility associated signaling (NFAS) E1 or T1 ISDN calls that arrive on B-channel 16 (for E1) or 24 (for T1) are not purged from the call history when the call disconnects; the calls are still shown as active. This situation can cause the ISDN process to consume large amounts of memory. This problem is resolved in Release 12.1(20)E. (CSCdv00338)
- A router may send linkUp traps with the loclfReason attribute set as “Down” and linkDown traps with the loclfReason attribute set as “Up.” This problem is resolved in Release 12.1(20)E. (CSCdv46906)
- The CISCO-MEMORY-POOL-MIB gives the wrong value for ciscoMemoryPoolType. This problem is resolved in Release 12.1(20)E. (CSCdv55144)
- The counters in the **show ip ospf** output are not being reset correctly when the process is cleared. This problem is resolved in Release 12.1(20)E.(CSCdv63847)
- When you enter the **ip tcp path-mtu-discovery** command on a router connected to an MPLS network, the BGP session times out. This problem is resolved in Release 12.1(20)E. (CSCdv89098)
- OSPF might not set nonzero forwarding address in external default LSA. This problem is resolved in Release 12.1(20)E. (CSCdw47949)
- If an IPsec peer receives an ISAKMP keepalive packet while keepalive is not locally configured on the router, the following message is generated:

  ```
  %SYS-3-MGDTIMER traceback
  ```

  This problem is resolved in Release 12.1(20)E. (CSCdw58489)
- The connectionless network service (CLNS) to DecNet translation process causes packet corruption. This problem is resolved in Release 12.1(20)E. (CSCdw79785)
- CLNS routes are not advertised on aggregation routers. This problem is resolved in Release 12.1(20)E. (CSCdw83966)
- When OSPF is redistributed into any distance vector protocol such as RIP or EIGRP, OSPF does not correctly process the command to remove the network. This problem is resolved in Release 12.1(20)E. (CSCdx17429)
- IOS server load balancing (SLB) does not inspect RADIUS attributes before destroying the framed-IP sticky database object. This problem is resolved in Release 12.1(20)E. (CSCdx70212)
- The multicast route monitor (MRM) test receiver intermittently reports false packet loss. This problem is resolved in Release 12.1(20)E. (CSCdy03612)
- Distance vector multicast routing protocol (DVMRP) does not advertise the proper routes. This problem is resolved in Release 12.1(20)E. (CSCdz08348)

- The following system message, which indicates an HSRP misconfiguration, is sent out as three separate messages instead of a single message:

  ```
  %STANDBY-3-DIFFVIP1
  ```

  This problem is resolved in Release 12.1(20)E. (CSCdz44758)
- Systems network architecture switching services (SNASw) logical units (LUs) may fail to establish a session with their virtual telecommunications access method (VTAM) application. This failure indicates that an intermediate or destination node was unable to successfully complete the processing of a high-performance routing (HPR) route-setup request or reply. This problem is resolved in Release 12.1(20)E. (CSCea09001)
- The **show extended channel** command causes 95 percent channel interface processor (CIP) utilization. This problem is resolved in Release 12.1(20)E. (CSCea28472)
- OpenView Monitoring SDLC traps generate messages for unknown SDLC links. This problem is resolved in Release 12.1(20)E. (CSCea34094)
- The SNASw router reloads when processing an internal command. This problem is resolved in Release 12.1(20)E. (CSCea36624)
- The running configuration does not show changes in the network time protocol (NTP) password. This problem is resolved in Release 12.1(20)E. (CSCea46073)
- Network-based application recognition (NBAR) does not work for the routing table protocol (RTP). This problem is resolved in Release 12.1(20)E. (CSCea56638)
- The **snasw stop ipstrace** command does not stop IPS tracing. This problem is resolved in Release 12.1(20)E. (CSCea78341)
- When you add a /31 netmask route, the new netmask does not overwrite an existing /32 CEF entry. This problem is resolved in Release 12.1(20)E. A facility has been provided to periodically validate prefixes derived from adjacencies in the FIB against prefixes originating from the RIB. To enable the validation, you must enter the **ip cef table adjacency-prefix validate** global configuration command. (CSCea53765)
- Multicast traffic is process switched after OIR. This problem is resolved in Release 12.1(20)E. (CSCea80221)
- The switch might drop into ROMMON mode after reload. This problem is resolved in Release 12.1(20)E. (CSCea88910)
- On a system with a Supervisor Engine 2, a MSFC 2 and a DFC, when the DFC card is reset, traffic is software switched for those ports that have HSRP enabled. This problem is resolved in Release 12.1(20)E. (CSCea89099)
- If you replace a WS-X6148-GE-TX or WS-X6148V-GE-TX switching module with a WS-X6548-GE-TX or WS-X6548V-GE-TX switching module, any **switchport** commands configured on the WS-X6148-GE-TX or WS-X6148V-GE-TX switching module do not work on the WS-X6548-GE-TX or WS-X6548V-GE-TX switching module. This problem is resolved in Release 12.1(20)E. (CSCea89432)
- When you configure interface speed and duplex mode, you must configure speed before you can configure the duplex mode. The speed and duplex mode configuration is stored in the configuration file in reverse order, which causes duplex mode configuration failure if you paste in a configuration file. This problem is resolved in Release 12.1(20)E. (CSCea93829)
- When a Cisco IOS server load balancing (Cisco IOS SLB) virtual server is configured for RADIUS load balancing with the **msid-cisco** keyword, then Accounting-Start RADIUS requests from a Home Agent may not be load-balanced to the same real server as the Access-Request. This problem is resolved in Release 12.1(20)E. (CSCeb00351)

- Deny ACEs that do not specify any Layer 4 ports incorrectly do not deny fragmented packets. This problem is resolved in Release 12.1(20)E. (CSCeb04343)
- An IEEE 802.Q trunking Gigabit EtherChannel formed with interfaces on different DFC-equipped switching modules might drop some traffic that is Layer 3 switched in hardware or that is routed in software. This problem is resolved in Release 12.1(20)E. (CSCeb05464)
- When the maximum number of RLB sticky subscribers for a real server (SSG1) are exceeded, the RLB does not pass AcctStop packets (from GGSN) to SSG1 for the existing host objects, but to the next SSG in the round-robin pool. The SSG proxies the AcctStop packets to the AAA server, which then closes the corresponding RADIUS sessions. This situation leads to stale host objects on the first SSG. This problem is resolved in Release 12.1(20)E. (CSCeb09340)
- Multicast shortcuts take a long time to install during dense mode fallback, which causes latency in hardware switching. This problem is resolved in Release 12.1(20)E. (CSCeb14435)
- With a Supervisor Engine 2, the IOS ARP and adjacency entries for the next-hop IP address configured for a static route might not be created. This problem is resolved in Release 12.1(20)E. (CSCeb38062)
- Supervisor Engine 1 does not have RP-SP inband channel communication monitoring. This problem is resolved in Release 12.1(20)E. (CSCeb46610)
- On WS-X6548-GE-TX and WS-X6548V-GE-TX modules, CEF-switched Ethernet egress packets that are less than 64-bytes long are not padded correctly. This problem is resolved in Release 12.1(20)E. (CSCeb47640)
- A memory leak might occur with Layer 2 aging and EtherChannels that include ports on different DFC-equipped modules configured. This problem is resolved in Release 12.1(20)E. (CSCeb48732)
- With RPR redundancy configured, the MSFC and OSMs might incorrectly reload. This problem is resolved in Release 12.1(20)E. (CSCeb49134)
- The CEF entries for traffic from a directly connected Layer 3 address are removed and recreated randomly, which causes Unicast traffic loss for the affected entries. This problem is resolved in Release 12.1(20)E. (CSCeb53542)
- There might be OSPF neighbor drops and HSRP flaps when QoS is enabled on a Supervisor Engine 1 and MSFC2. This problem is resolved in Release 12.1(20)E. (CSCeb55271)
- With a redundant supervisor engine installed, the configuration of EtherChannels that are reconfigured from Layer 2 to Layer 3 is not synchronized to the redundant supervisor engine. This problem is resolved in Release 12.1(20)E. (CSCeb56353)
- Memory usage when handling route flaps is not optimal, which causes the route-flap handling process to hold memory longer than necessary and which can cause out-of-memory conditions when routes flap continuously. This problem is resolved in Release 12.1(20)E. (CSCeb57465)
- Incorrect VTP pruning might occur if you delete or rename VLANs in VLAN database mode. This problem is resolved in Release 12.1(20)E. (CSCeb60262)
- The 64-bit SNMP counters on OSM-4GE-WAN and OSM-2+4GE-WAN+ modules behave like 32-bit counters. This problem is resolved in Release 12.1(20)E. (CSCeb60961)
- When the multicast traffic level exceeds the Layer 3 hardware switching capacity, the excess multicast traffic might be dropped instead of being routed in software on the MSFC. This problem is resolved in Release 12.1(20)E. (CSCeb62692)
- If you enter the **shutdown** command and then the **no shutdown** command on an interface that is handling a high volume of Layer 3 hardware switched multicast traffic, some of the multicast traffic is routed in software on the MSFC instead of being Layer 3 switched in hardware when the interface comes back up. This problem is resolved in Release 12.1(20)E. (CSCeb67996)

- With QoS and Cisco IOS server load balancing (Cisco IOS SLB) configured on a Supervisor Engine 1, a VACL configured to filter multicast traffic on one VLAN might incorrectly be applied to multicast traffic on other VLANs. This problem is resolved in Release 12.1(20)E. (CSCeb69582)
- OIR of a fabric-enabled switching module might cause a reload. This problem is resolved in Release 12.1(20)E. (CSCec12236)
- A reload might occur if you modify a policy map that is attached to an interface. This problem is resolved in Release 12.1(20)E. (CSCec15119)
- With EoMPLS configured, a reload might occur if you configure a different access VLAN on the CE-facing port. This problem is resolved in Release 12.1(20)E. (CSCec23787)
- With a large number of static multicast entries configured (approximately 8,000), some entries might not propagate to DFCs. This problem is resolved in Release 12.1(20)E. (CSCec50577)
- With the Protocol Independent Multicast (PIM) Dense-Mode State Refresh feature enabled, a reload might occur if the group mode changes from PIM dense mode to PIM sparse or bidirectional mode. This problem is resolved in Release 12.1(20)E. (CSCea09302)
- After a Systems Network Architecture (SNA) physical unit (PU) has been disconnected for several hours and then reconnected, the physical unit fails to connect when using Data Link Switching (DLSw) Ethernet Redundancy (ER) with transparent map statements. This problem is resolved in Release 12.1(20)E. (CSCeb02695)
- The Cisco IOS DHCP server does not send a DHCPNAK message when it receives a broadcast DHCPREQUEST message from a DHCP client that has moved from one subnet to another. This problem is resolved in Release 12.1(20)E. (CSCeb33403)
- If you enter a **show interface etherchannel** command or a **show interface etherchannel module** command for an EtherChannel with ports on a module that is no longer installed, the MSFC might reload or there might be a switchover to a redundant supervisor engine. This problem is resolved in Release 12.1(20)E. (CSCeb53215)
- Loss of a fan, either through failure or because of power supply shutdown, might cause a reload. This problem is resolved in Release 12.1(20)E. (CSCeb51698)
- When you save the configuration, the following spurious message appears:

  ```
  %This controller does not support APS[OK]
  ```

  This problem is resolved in Release 12.1(20)E. (CSCin43261)

FlexWAN Caveats

- Open FlexWAN Caveats in Release 12.1(20)E6, page 207
- Resolved FlexWAN Caveats in Release 12.1(20)E6, page 208
- Resolved FlexWAN Caveats in Release 12.1(20)E3, page 208
- Resolved FlexWAN Caveats in Release 12.1(20)E2, page 208
- Resolved FlexWAN Caveats in Release 12.1(20)E, page 208

Open FlexWAN Caveats in Release 12.1(20)E6

None.

Resolved FlexWAN Caveats in Release 12.1(20)E6

- Serial interfaces on a PA-MC-8TE1+ port adapter that are configured as part of a channel group continue to process packets when the interface is in the "admindown" state. The counters in the output of the **show interfaces serial** command might increment when the serial interface is shut down. This problem is resolved in Release 12.1(20)E6. (CSCin78325)

Resolved FlexWAN Caveats in Release 12.1(20)E3

- Operation, Administration, and Maintenance (OAM) permanent virtual circuits (PVC) on PA-A3-8T1IMA or PA-A3-8E1IMA interfaces are not active after an OIR. This problem is resolved in Release 12.1(20)E3. (CSCin65182)
- An administratively shut-down subinterface that is configured for Frame-Relay encapsulation might forward packets. This problem is resolved in Release 12.1(20)E3. (CSCed78803)
- With heavy traffic through a PA-MC-T3 or PA-MC-E3 port adapter, a FlexWAN module might reload. This problem is resolved in Release 12.1(20)E3. (CSCin62978)
- With a high traffic load, PA-A3-OC3, PA-A3-T3, and PA-A3-E3 port adapters might display an increasing "rx_no_buffer" counter in the output of the **show controllers atm** privileged EXEC command and some PVCs configured on the PA-A3 port adapter might stop receiving traffic. This problem is resolved in Release 12.1(20)E3. (CSCin49458)

Resolved FlexWAN Caveats in Release 12.1(20)E2

- When EoMPLS virtual circuits (VCs) are loadbalanced across an OSM-2+4GE-WAN+ physical interface and a subinterface, the OSM reloads if you remove a service policy from the physical interface. This problem is resolved in Release 12.1(20)E2. (CSCec65147)
- Illegal memory accesses when a dGRE test is configured on HSSI Frame Relay encapsulation for a FlexWAN module might cause a reload. This problem is resolved in Release 12.1(20)E2. (CSCin29514)
- A FlexWAN module is not detected during the boot process causing it to be ignored during the startup configuration process. This problem is resolved in Release 12.1(20)E2. (CSCed00781)
- The FlexWAN module may reload when it is booting up. This problem is resolved in Release 12.1(20)E2. (CSCec55445)

Resolved FlexWAN Caveats in Release 12.1(20)E

- Ignore messages from a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) that reports a large number of degraded minutes on an E1 controller. For example, after 15 minutes of operation since startup, 35,000,000 degraded minutes might be reported and these values might increase every second. Code violations might also be reported. This problem is resolved in Release 12.1(20)E. (CSCec08973)
- When a Tributary Unit Alarm Indication Signal (TU-AIS) is inserted for an E1 tributary on a PA-MC-STM-1 port adapter in a Synchronous Payload Envelope (SPE), packet corruption might occur on the adjacent E1. This problem is resolved in Release 12.1(20)E. (CSCea66218)
- You can attach a service policy that contains invalid configuration to an interface. If you apply a Frame Relay map-class with both input policing and output queuing to a DLCI twice, the FlexWAN module might reload. This problem is resolved in Release 12.1(20)E. (CSCin52060)

- After a few weeks of normal operation, an interface on a PA- MC-8E1 port adapter begins flapping and finally pauses with the output queue stuck as follows:

```
Serial1/1:1 is up, line protocol is up
Encapsulation HDLC, crc 16, Data non-inverted
Keepalive set (120 sec)
Last input 00:00:03, output 04:14:23, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 21952
Queueing strategy: weighted fair
Output queue: 30/4000/64/21855 (size/max total/threshold/drops)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
43903807 packets input, 3646461183 bytes, 0 no buffer
Received 0 broadcasts, 321 runts, 0 giants, 0 throttles
5160 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 2945 abort
42026998 packets output, 2185017012 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets 0 output buffer failures,
0 output buffers swapped out 31 carrier transitions
no alarm present
Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags
```

  The following traceback is observed in the log:

```
%LINK-4-TOOBIG: Interface Serial60:1, Output packet size of 1526 bytes too big
Traceback= 0x604007F8 0x604A927C 0x6084E4D4 0x6057425C 0x60CE921C 0x60CE55EC
%LINK-4-TOOBIG: Interface Serial20:1, Output packet size of 1526 bytes too big
Traceback= 0x604007F8 0x604A927C 0x6084E4D4 0x6057425C 0x60CE921C 0x60CE55EC
```

  This problem is resolved in Release 12.1(20)E. (CSCdz72292)

- All high-capacity counters remain at 0 for FlexWAN module POS interfaces. This problem is resolved in Release 12.1(20)E. (CSCdz46845)
- Connections cannot be made to users behind ATM PVCs on a FlexWAN module. This problem is resolved in Release 12.1(20)E. (CSCdz61962)
- In a system installed with a FlexWAN and a PA-A3 ATM port adapter, the ATM interface may stay down after you enter a **shutdown** command followed immediately by a **no shutdown** command. This problem is resolved in Release 12.1(20)E. (CSCdy23751, CSCdw65799)
- With a redundant Supervisor Engine 2, crypto images do not recognize FlexWAN modules at bootup when RPR is configured. This problem is resolved in Release 12.1(20)E. (CSCeb47607)
- With dial-up networking (DUN) configured, the IP Control Protocol (IPCP) times out on a link control protocol (LCP) negotiation. This problem is resolved in Release 12.1(20)E. (CSCea51540)
- ATM subinterface traffic might be incorrectly dropped. This problem is resolved in Release 12.1(20)E. (CSCea81118

Service Module Caveats

- Open Service Module Caveats in Release 12.1(20)E6, page 210
- Resolved Service Module Caveats in Release 12.1(20)E6, page 210
- Resolved Service Module Caveats in Release 12.1(20)E3, page 210
- Resolved Service Module Caveats in Release 12.1(20)E2, page 210
- Resolved Service Module Caveats in Release 12.1(20)E, page 210

Open Service Module Caveats in Release 12.1(20)E6

None.

Resolved Service Module Caveats in Release 12.1(20)E6

None.

Resolved Service Module Caveats in Release 12.1(20)E3

None.

Resolved Service Module Caveats in Release 12.1(20)E2

- BPDU packets are not sent to Firewall Services Module (FWSM) ports. When transparent-firewall mode is used, this situation may cause packet-forwarding loops when redundancy is enabled or when two Firewall Services Modules share the same VLANs. This problem is resolved in Release 12.1(20)E2. (CSCec14054)

Resolved Service Module Caveats in Release 12.1(20)E

- The **analysis module** *slot_num* **data-port** *port_num* **capture** command that enables WS-SVC-NAM-2 or WS-SVC-IDSM2 data port capture is not synchronized to the redundant supervisor in RPR+ mode. This problem is resolved in Release 12.1(20)E. (CSCeb17522)
- A reload might occur following an RPR or RPR+ switchover if more than one service module is installed. This problem is resolved in Release 12.1(20)E. (CSCeb11966)
- A Catalyst 6509 switch with a Supervisor Engine 1 and an MSFC2 repeatedly reboots when an IDSM2 is installed. This problem is resolved in Release 12.1(20)E. (CSCeb30944)
- The Gigabit Ethernet ports on the OC-48 OSMs may experience output drops. This problem is resolved in Release 12.1(20)E. (CSCea76234)
- When an EoMPLS VC is configured on an OSM, the output counter and some interface MIB counters display incorrect values. This problem is resolved in Release 12.1(20)E. (CSCeb04036)

OSM Caveats

- Open OSM Caveats in Release 12.1(20)E6, page 210
- Resolved OSM Caveats in Release 12.1(20)E6, page 211
- Resolved OSM Caveats in Release 12.1(20)E3, page 211
- Resolved OSM Caveats in Release 12.1(20)E2, page 211
- Resolved OSM Caveats in Release 12.1(20)E, page 211

Open OSM Caveats in Release 12.1(20)E6

- DSCP class-based shaping might not work on ATM OSMs. (CSCed62252)

Note CSCed62252 is not seen in later releases.

Resolved OSM Caveats in Release 12.1(20)E6

None.

Resolved OSM Caveats in Release 12.1(20)E3

- OSM ATM interfaces do not support the SNMP lowerLayerDown value defined in RFC 2863. This problem is resolved in Release 12.1(20)E6. (CSCee56269)

Resolved OSM Caveats in Release 12.1(20)E2

- OSM-4GE-WAN interfaces remain in the "up/up" state when the other end of the link is inactive. This problem is resolved in Release 12.1(20)E2. (CSCec79460)
- If you delete and recreate Frame Relay subinterfaces in random order on OSM POS interfaces, some traffic might be sent to the wrong subinterface. This problem is resolved in Release 12.1(20)E2. (CSCec67501)
- Directed broadcasts to a destination network that is part of an MPLS VPN fail.This problem is resolved in Release 12.1(20)E2. (CSCec75499)
- Parallel Express Forwarding (PXF) CEF load balancing does not work. This problem is resolved in Release 12.1(20)E2. (CSCdu47678)
- Distributed CEF switching does not work for multilink interface egress traffic. This problem is resolved in Release 12.1(20)E2. (CSCec55650)
- The serial interface input and output counters for an OSM always show 0 when you enter the **show interfaces serial** command. This problem is resolved in Release 12.1(20)E2. (CSCed07367)
- The 64-bit counter on the OSM-2+4GE-WAN+ main interface shows an incorrect value of zero. This problem is resolved in Release 12.1(20)E2. (CSCec34010)
- An OC-12 POS OSM might reset as a result of memory corruption. This problem is resolved in Release 12.1(20)E2. (CSCec59550)

Resolved OSM Caveats in Release 12.1(20)E

- Exported NetFlow counts are less than the actual value when parallel express forwarding (PXF) is enabled. This problem is resolved in Release 12.1(20)E. (CSCea45873)
- On OSMs, Cisco IOS software disables some GBICs when the software incorrectly reports that the GBIC has a faulty EEPROM instead of type 25 or type 29 media ("unknown media type"). This problem is resolved in Release 12.1(20)E. (CSCeb86171)
- Because subinterfaces on the OSM-2+4GE-WAN+ module cannot share HSRP group numbers, the 4-port Gigabit Ethernet WAN module supports only 16 HSRP groups per Gigabit Ethernet WAN port. This problem is resolved in Release 12.1(20)E. (CSCeb11624)
- When TTL propagation has been turned off by entering the **tag-switching ip propagate-ttl** command, MPLS TTLs are still copied to IP packets. This problem is resolved in Release 12.1(20)E. (CSCdy47341)
- A Catalyst 6509 with an OSM module installed experiences a drop in output on the Gigabit Ethernet port when you connect another device to that port. This problem is resolved in Release 12.1(20)E. (CSCdz62748)
- An ATM OSM module does not route packets between bridged RFC 1483 PVCs that are configured in different VLANs. This problem is resolved in Release 12.1(20)E. (CSCea84940)

- The PE does not map IP DSCP to the MPLS experimental field in the output interface. By default, the router copies the three most significant bits of the DSCP of the IP packet to the EXP field in the MPLS shim header. This problem is resolved in Release 12.1(20)E. (CSCea87671)
- OSM interfaces may stop receiving data after an RPR+ switchover. This problem is resolved in Release 12.1(20)E. (CSCeb42402)
- For virtual private dial-up networks (VPDN), when an L2TP access concentrator (LAC) negotiates an authentication protocol that is not listed as a valid authentication protocol according to the L2TP Network Server (LNS) configuration, the LNS incorrectly accepts the negotiated options and uses the authentication protocol set by the LAC. This problem is resolved in Release 12.1(20)E. (CSCdz83019)
- EoMPLS VCs flap on an 8-port, 8 Gbps customer edge-to-provider edge (CE-to-PE) router connection between WS-X6516-GBIC and OSM-2+4GE-WAN+ modules. This problem is resolved in Release 12.1(20)E. (CSCeb04954)
- The FIB on an OSM might not be synchronized with the FIB on the MSFC. This problem is resolved in Release 12.1(20)E. (CSCeb52142)
- When an OSPF topology change occurs, an MPLS provider edge (PE) router might not forward IP-to-Tag traffic to some IP destinations when it has equal cost load-sharing paths to the IP destinations. This problem is resolved in Release 12.1(20)E. (CSCeb52169)
- The **set mpls exp** and **set ip precedence** commands are not supported with basic MPLS and MPLS VPN. This problem is resolved in Release 12.1(20)E. (CSCin43408, CSCeb25018)
- An E3 link to an OC-12 channelized OSM might not come up. This problem is resolved in Release 12.1(20)E. (CSCec39689)

Release 12.1(19)E and Rebuilds

Note Release 12.1(19)E1a images are posted on the LAN Switching Software page at this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-sup-ios

Release 12.1(19)E1a images are not posted on the Cisco IOS Upgrade Planner page.

- General Caveats, page 212
- FlexWAN Caveats, page 217
- Service Module Caveats, page 218
- OSM Caveats, page 218

General Caveats

- Open General Caveats in Release 12.1(19)E1a, page 213
- Resolved General Caveats in Release 12.1(19)E1a, page 213
- Resolved General Caveats in Release 12.1(19)E1, page 213
- Resolved General Caveats in Release 12.1(19)E, page 214

Open General Caveats in Release 12.1(19)E1a

None.

Resolved General Caveats in Release 12.1(19)E1a

- Routing protocols do not work on EtherChannels that are reconfigured from Layer 2 to Layer 3. This problem is resolved in Release 12.1(19)E1a. (CSCeb60132, CSCeb07123)
- A global command is needed for enabling link state messages on interfaces. This problem is resolved in Release 12.1(19)E1a. (CSCeb06765)
- After a Systems Network Architecture (SNA) physical unit (PU) has been disconnected for several hours and then reconnected, the physical unit fails to connect when using Data Link Switching (DLSw) Ethernet Redundancy (ER) with transparent map statements. This problem is resolved in Release 12.1(19)E1a. (CSCeb02695)
- The Cisco IOS DHCP server does not send a DHCPNAK message when it receives a broadcast DHCPREQUEST message from a DHCP client that has moved from one subnet to another. This problem is resolved in Release 12.1(19)E1a. (CSCeb33403)
- If you enter a **show interface etherchannel** command or a **show interface etherchannel module** command for an EtherChannel with ports on a module that is no longer installed, the MSFC might reload or there might be a switchover to a redundant supervisor engine. This problem is resolved in Release 12.1(19)E1a. (CSCeb53215)
- Loss of a fan, either through failure or because of power supply shutdown, might cause a reload. This problem is resolved in Release 12.1(19)E1a. (CSCeb51698)
- When you save the configuration, the following spurious message appears:

  ```
  %This controller does not support APS[OK]
  ```

  This problem is resolved in Release 12.1(19)E1a. (CSCin43261)

Resolved General Caveats in Release 12.1(19)E1

- A memory leak might occur with Layer 2 aging and EtherChannels that include ports on different DFC-equipped modules configured. This problem is resolved in Release 12.1(19)E1. (CSCeb48732)
- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.1(19)E1. (CSCdu53656)
- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

This problem is resolved in Release 12.1(19)E1. (CSCea28131)

- You cannot use a named aggregate policer and a microflow policer together if both are configured to set the same IP precedence value for conforming traffic. This problem is resolved in Release 12.1(19)E1. (CSCeb22674)
- Static multicast router port configuration is not in effect following a reload. This problem is resolved in Release 12.1(19)E1. (CSCea93328)
- When you configure Cisco IOS server load balancing (Cisco IOS SLB), MLS long aging does not work. This problem is resolved in Release 12.1(19)E1. (CSCea83612)
- When you remove a module, an unnecessary message is printed that says the interfaces on the removed module have been disabled. This problem is resolved in Release 12.1(19)E1. (CSCdz77879)
- A router that is not the RP for a group and that gets a periodic (*,G) join message with an SGR prune message might process the (*,G) join message before seeing the SGR prune message and incorrectly send only a (*,G) join to the RP. This problem is resolved in Release 12.1(19)E1. (CSCea13379)
- The switch might drop into ROMMON mode after reload. This problem is resolved in Release 12.1(19)E1. (CSCea88910)
- When the maximum number of RLB sticky subscribers for a real server (SSG1) are exceeded, the RLB does not pass AcctStop packets (from GGSN) to SSG1 for the existing host objects, but to the next SSG in the round-robin pool. The SSG proxies the AcctStop packets to the AAA server, which then closes the corresponding RADIUS sessions. This situation leads to stale host objects on the first SSG. This problem is resolved in Release 12.1(19)E1. (CSCeb09340)
- Multicast shortcuts take a long time to install during dense mode fallback, which causes latency in hardware switching. This problem is resolved in Release 12.1(19)E1. (CSCeb14435)
- A default route learned through a routing protocol might be either missing or incomplete. This problem is resolved in Release 12.1(19)E1. (CSCeb18552)

Resolved General Caveats in Release 12.1(19)E

- NAT receives traffic translated by itself. This problem is resolved in Release 12.1(19)E. (CSCdz18109)
- A manually summarized entry might remain in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table after manual summarization is disabled. This problem is resolved in Release 12.1(19)E. (CSCdx83729)
- OSPF might set the partial database flag without a partial shortest path first (SPF) ever happening when a link-state advertisement (LSA) update received from a neighbor has a different mask from the mask in previous LSA updates, which might prevent the LSA from being deleted from the OSPF database. This problem is resolved in Release 12.1(19)E. (CSCdz82284)
- MPLS does not work if you configure fall-back bridging on the MPLS subinterface. This problem is resolved in Release 12.1(19)E. (CSCdz75507; see resolved caveats CSCeb87433 and CSCee00239)
- A reload might occur when a TCP session is cleared. This problem is resolved in Release 12.1(19)E. (CSCdw76948)
- A CPU hog condition might cause a reload when the **snmp-server community** global configuration command is executed with several thousands of logical entities configured. This problem is resolved in Release 12.1(19)E. (CSCdx68230)

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

  This problem is resolved in Release 12.1(19)E. (CSCdz71127)

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

  This problem is resolved in Release 12.1(19)E. (CSCea02355)

- Incorrect flooding might occur in a 13-slot chassis with DFCs. This problem is resolved in Release 12.1(19)E. (CSCeb11577)
- You can incorrectly configure a less-specific flowmask when you have features configured that require a more-specific flowmask. This problem is resolved in Release 12.1(19)E. (CSCea86541)
- In a topology that uses VLAN interfaces for intermediate router connections, PIM register and PIM register stop messages might loop between the intermediate routers until the TTL count expires. This problem is resolved in Release 12.1(19)E. (CSCea82353)
- Hardware failures on the WS-X6548-RJ-45 module are not detected. This problem is resolved in Release 12.1(19)E. (CSCea73615)
- With the fastest aging time configured and the highest flow creation rates configured, the statistics exported by NetFlow data export are not accurate. The inaccuracy is reduced in Release 12.1(19)E. (CSCea72771)
- When using stateful Cisco IOS SLB and with the standby preempt command configured on some interfaces, a switchover to the redundant supervisor engine might cause high CPU utilization. This problem is resolved in Release 12.1(19)E. (CSCea54756)
- With IP inspection configured, a reload might occur following an “%ALIGN-1-FATAL” message. This problem is resolved in Release 12.1(19)E. (CSCea51320)
- Hardware-supported ACLs without any ACEs do not implicitly deny all traffic. This problem is resolved in Release 12.1(19)E. (CSCea17192)
- A reload might occur if you configure an IP address that is a duplicate of an IP address configured on a redistributed BGP peer. This problem is resolved in Release 12.1(19)E. (CSCdz30644)
- Following loss of the link to the PBR next hop, the new next hop information is not programmed into hardware immediately. This problem is resolved in Release 12.1(19)E. (CSCdy28888)

- An MSFC2 might reload with the following error messages:

  ```
  MISTRAL-3-ERROR: Error condition detected: SYSAD_TIMEOUT_DPATH
  ```

  and:

  ```
  sysad_dpath_addr_log = 0x100002E1
  ```

  This problem is resolved in Release 12.1(19)E. (CSCdu83548)
- With PIM dense mode configured, multicast traffic might get dropped when all routers have the multicast group in a pruned state even though interested receivers are present. This problem is resolved in Release 12.1(19)E. (CSCea26993)
- When you insert an SFM and cause a transition to truncated mode, QoS policing and marking stop working. This problem is resolved in Release 12.1(19)E. (CSCeb09034)
- Web sites that require authentication become unreachable. This symptom is observed on an MSFC on which Web Cache Communication Protocol (WCCP) is enabled and Cisco Express Forwarding (CEF) switching is disabled. This problem is resolved in Release 12.1(19)E. (CSCdz36099)
- No command exists to disable the generation of PPP Link Control Protocol (LCP) keepalive failure link-down traps. These traps are sent by default when the LCP goes down. This problem is resolved in Release 12.1(19)E with the introduction of the new **no ppp link trap** command. (CSCdy05898)
- An interface that is defined in an Enhanced Interior Gateway Routing Protocol (EIGRP) network statement may fail to come up in the EIGRP topology table. This symptom is observed after a system reload. The occurrence of the symptom depends on the type of interface that is connected and on the timing of the interface activation. This problem is resolved in Release 12.1(19)E. (CSCdz41087)
- The system may reload unexpectedly when saving the configuration to NVRAM. This symptom is observed in a system that is configured with the **service compress-config global** configuration command. This problem is resolved in Release 12.1(19)E. (CSCdz32940)
- A window condition may occur if an initial program load (IPL) is performed on a mainframe while it is processing a primary logical unit secondary logical unit (PLU-SLU) session over a dependent logical unit requester (DLUR). A logical unit (LU) may hang and may cause a downstream physical unit (DSPU) to pause indefinitely. The DSPU state is shown as “reset” even though the finite state machine (FSM) history shows the DSPU state as “reset link inactive.” The state of the LU is also reset, and the DSPU cannot be used. An IPL has to be performed on the Systems Network Architecture (SNA) switch to recover the DSPU. These symptoms are observed only in a small window condition when an IPL is performed on a host while DLUR is used. This problem is resolved in Release 12.1(19)E. (CSCdx77062)
- UP and DOWN status messages may be displayed on the console. This symptom is observed when a leased-line configuration is in the UP state, but the peer is not responding. This symptom occurs because PPP calls the interface reset vector regularly if the peer is not responding to the PPP attempts to communicate. This problem is resolved in Release 12.1(19)E. (CSCdx55880)
- TCP processing fails in the data repacketized process and creates inaccurate packets. A data-link switching (DLSw) circuit disconnects suddenly, and the following error message is displayed if you enter the **debug dlsw core** command on one for the DLSW routers:

  ```
  DLSW: Invalid dlsw version 78
  ```

  The number 78 is an example and may be any other number. These symptoms are observed during an attempted TCP retransmission of a message and TCP data packet reconstruction on a DLSw router. This problem is resolved in Release 12.1(19)E. (CSCdx55357)
- A Systems Network Architecture Switching Services (SNASw) router that is configured with a downstream port of conntype=len incorrectly advertises itself as nodetype=NN in the exchange identification (XID) exchange. This problem is resolved in Release 12.1(19)E. (CSCdx47521)

- A redundant supervisor engine might not reload if you enter the reload command on the redundant supervisor engine's console or physically remove and reinsert the redundant supervisor engine. This problem is resolved in Release 12.1(19)E. (CSCea66858)
- When not configured with a redundant power supply, continuous reloads might happen if the output from the single power supply is momentarily unstable, which causes this message to be displayed:

  ```
  "%C6KPWR-2-INSUFFICIENTPOWER: Powering down all linecards as there is not enough power
  to operate all critical cards"
  ```

  This problem is resolved in Release 12.1(19)E. (CSCea82777)

FlexWAN Caveats

- Open FlexWAN Caveats in Release 12.1(19)E1a, page 217
- Resolved FlexWAN Caveats in Release 12.1(19)E1a, page 217
- Resolved FlexWAN Caveats in Release 12.1(19)E1, page 217
- Resolved FlexWAN Caveats in Release 12.1(19)E, page 218

Open FlexWAN Caveats in Release 12.1(19)E1a

- In a system installed with a FlexWAN and a PA-A3 ATM port adapter, the ATM interface may stay down after you enter a **shutdown** command followed immediately by a **no shutdown** command.

  Workaround: After you enter the **shutdown** command on the interface, wait for 1 minute before entering the **no shutdown** command. This problem is resolved in Release 12.1(20)E. (CSCdy23751, CSCdw65799)

Resolved FlexWAN Caveats in Release 12.1(19)E1a

- Spurious memory accesses in cwpa_1483_bridge_vlan_pvc_egress_classify occur following a reload. This problem is resolved in Release 12.1(19)E1a. (CSCin39391)
- With modular QoS CLI (MQC) fragmentation and shaping configured on a FlexWAN Frame Relay interface, the FlexWAN module might pause indefinitely, produce large numbers of spurious memory accesses, or reload; and produce messages reporting that the FlexWAN interfaces are not sending packets and that the output of the interfaces is stuck. This problem is resolved in Release 12.1(19)E1a. (CSCeb22972, CSCeb00104)

Resolved FlexWAN Caveats in Release 12.1(19)E1

- With a redundant Supervisor Engine 2, crypto images do not recognize FlexWAN modules at bootup when RPR is configured. This problem is resolved in Release 12.1(19)E1. (CSCeb47607)
- With dial-up networking (DUN) configured, the IP Control Protocol (IPCP) times out on a link control protocol (LCP) negotiation. This problem is resolved in Release 12.1(19)E1. (CSCea51540)
- The counters in the show interfaces command for FlexWAN interfaces are not accurate. This problem is resolved in Release 12.1(19)E1. (CSCea06360)
- A reload might occur when you configure an ATM bundle. This problem is resolved in Release 12.1(19)E1. (CSCeb03367)

Resolved FlexWAN Caveats in Release 12.1(19)E

- When you configure IP precedence to ATM CoS mapping in a bundle on a FlexWAN ATM port adapter, the precedence mapping does not work if you specify a range of precedences under a VC in the bundle. The bundle only forwards the first precedence in the range. This problem is resolved in Release 12.1(19)E. (CSCea56687)
- After a reload, some PVCs on PA-A3-8T1/8E1 IMA port adapter interfaces might remain inactive. This problem is resolved in Release 12.1(19)E. (CSCin33669)
- Operation, Administration, and Maintenance (OAM)-managed permanent virtual circuits (PVCs) on an 8-port T1 ATM port adapter with IMA (PA-A3-8T1IMA) or on an 8-port E1 ATM port adapter with IMA (PA-A3-8E1IMA) may not come up as expected. This problem is resolved in Release 12.1(19)E. (CSCdy36665)
- A reload might occur if there are multiple sessions configuring an ATM interface at the same time. This problem is resolved in Release 12.1(19)E. (CSCdr61944)
- VPN does not work on multilink PPP (MLPPP) interfaces. This problem is resolved in Release 12.1(19)E. (CSCea37725)

Service Module Caveats

- Open Service Module Caveats in Release 12.1(19)E1a, page 218
- Resolved Service Module Caveats in Release 12.1(19)E1a, page 218
- Resolved Service Module Caveats in Release 12.1(19)E1, page 218
- Resolved Service Module Caveats in Release 12.1(19)E, page 218

Open Service Module Caveats in Release 12.1(19)E1a

None.

Resolved Service Module Caveats in Release 12.1(19)E1a

None.

Resolved Service Module Caveats in Release 12.1(19)E1

- VLAN SNMP ifIndexes are not sent to a NAM. This problem is resolved in Release 12.1(19)E1. (CSCeb05818)

Resolved Service Module Caveats in Release 12.1(19)E

- Except when using the console connection, a reload might occur when you try to configure a WS-X6066-SLB-APC module. This problem is resolved in Release 12.1(19)E. (CSCeb00678)
- The VLAN autostate behavior is not correct with a WS-SVC-NAM-2 module installed and configured. This problem is resolved in Release 12.1(19)E. (CSCea71694)

OSM Caveats

- Open OSM Caveats in Release 12.1(19)E1a, page 219
- Resolved OSM Caveats in Release 12.1(19)E1a, page 219

- Resolved OSM Caveats in Release 12.1(19)E1, page 219
- Resolved OSM Caveats in Release 12.1(19)E, page 220

Open OSM Caveats in Release 12.1(19)E1a

- After an OSM-4GE-WAN module resets, this message is displayed:

```
Mar  1 16:06:15.729: SP: TCAM ASSERT FAILURE:
label_alloc_tbl[label].num_if_using[lookup_type] !=
0: ../const/native-sp/tcam_label.c: 1379
Mar  1 16:06:15.733: SP: -Traceback= 403D5140 403C2368 403C09A0 403C27D8 403C73E0
403C84B4 403C8708 400F63D4 400F63C0
```

(CSCed87582)

Note CSCed87582 is not seen in later releases.

Resolved OSM Caveats in Release 12.1(19)E1a

- The OSM-12CT3/T1 interfaces have incorrect timing of the 15-minute intervals used to accumulate performance statistics and incorrectly do not accumulate 96 intervals. This problem is resolved in Release 12.1(19)E1a. (CSCeb54936)
- The interface rate counters on OSM-12CT3/T1 interfaces that are part of a multilink bundle do not increment. This problem is resolved in Release 12.1(19)E1a. (CSCeb54698)
- An OSM-2OC48/1DPT module only transmits egress multicast traffic through side A. This problem is resolved in Release 12.1(19)E1a. (CSCdz90594)
- In a DPT ring topology, nonRPF multicast traffic received on the DPT interface might cause a high CPU load. This problem is resolved in Release 12.1(19)E1a. (CSCeb45403)

Resolved OSM Caveats in Release 12.1(19)E1

- OSM interfaces may stop receiving data after an RPR+ switchover. This problem is resolved in Release 12.1(19)E1. (CSCeb42402)
- A Catalyst 6509 switch with a Supervisor Engine 1 and an MSFC2 repeatedly reboots when an IDSM2 is installed. This problem is resolved in Release 12.1(19)E1. (CSCeb30944)
- An ATM OSM module does not route packets between bridged RFC 1483 PVCs that are configured in different VLANs. This problem is resolved in Release 12.1(19)E1. (CSCea84940)
- For virtual private dial-up networks (VPDN), when an L2TP access concentrator (LAC) negotiates an authentication protocol that is not listed as a valid authentication protocol according to the L2TP Network Server (LNS) configuration, the LNS incorrectly accepts the negotiated options and uses the authentication protocol set by the LAC. This problem is resolved in Release 12.1(19)E1. (CSCdz83019)
- A reload occurs when you enter the **clear counter** command on a OSM-2OC48/1DPT module interface. This problem is resolved in Release 12.1(19)E1. (CSCeb21292)
- You might not be able to configure F4 VCs for ATM PVPs on an OSM-2OC12-ATM interface. This problem is resolved in Release 12.1(19)E1. (CSCeb31997)
- You cannot set the MPLS EXP bits with a service policy attached to an EoMPLS VLAN. This problem is resolved in Release 12.1(19)E1. (CSCeb29441)

- You cannot change the high priority queue rate for an OSM SRP interface. This problem is resolved in Release 12.1(19)E1. (CSCeb18943)
- If you remove a service policy from an OSM interface where EoMPLS traffic is flowing, the OSM might reload. This problem is resolved in Release 12.1(19)E1. (CSCin33060)
- Occasionally, OSM POS interfaces stop updating statistics while traffic is passing. This problem is resolved in Release 12.1(19)E1. (CSCea78519)

Resolved OSM Caveats in Release 12.1(19)E

- CBWFQ and LLQ policies are not applied to packets at the provider edge (PE) router's outgoing interface. This problem is resolved in Release12.1(19)E. (CSCdv82519)
- A shaping policy cannot be applied as the output service policy for EoMPLS VLANs. This problem is resolved in Release12.1(19)E. (CSCea72468)
- EoMPLS disposition traffic is not excluded from PFC VLAN policing. This problem is resolved in Release12.1(19)E. (CSCdy50772)
- A software condition may cause a router to reload, and a "%SYS-3- OVERRUN" error message may be generated. This symptom is observed on a system running Parallel Express Forwarding (PXF). The symptom is more likely to occur during periods of congestion. This problem is resolved in Release 12.1(19)E. (CSCdy68922)
- A reload might occur if there are multiple sessions configuring an ATM interface at the same time. This problem is resolved in Release 12.1(19)E. (CSCdr61944)

Release 12.1(14)E

Note All images in Release 12.1(14)E have been deferred.

- General Caveats, page 220
- FlexWAN Module Caveats, page 224
- Service Modules Caveats, page 225
- OSM Caveats, page 225

General Caveats

- Open General Caveats in Release 12.1(14)E, page 221
- Resolved General Caveats in Release 12.1(14)E, page 221

Open General Caveats in Release 12.1(14)E

- Routing protocols do not work on EtherChannels that are reconfigured from Layer 2 to Layer 3. This problem is resolved in Release 12.1(19)E1a. (CSCeb60132, CSCeb07123)

Resolved General Caveats in Release 12.1(14)E

Note In Release 12.1(14)E, caveat CSCdy36604 disabled SNMP retrieval of dot1dBase group data on VLANs where the spanning tree protocol is not enabled. Caveat CSCdy36604 conflicts with RFC 1493 and the effect of caveat CSCee39798 in Release 12.1(23)E.

- With a Supervisor Engine 2, (*,G) multicast entries are not programmed in hardware. This problem is resolved in Release 12.1(14)E. (CSCdy44937)
- Cisco IOS server load balancing (Cisco IOS SLB) connectivity might fail following a "%ICC-SP-5-WATERMARK" message. This problem is resolved in Release 12.1(14)E. (CSCdy37563)
- When multiple switches create a loop that is blocked by STP at the SSG and there is a link failure and recovery on the primary forwarding link between the RLB and the SSG, traffic stops until the MAC address age timer expires. This problem is resolved in Release 12.1(14)E. (CSCdy34266)
- MAC addresses with the routed MAC bit set (Routed MAC part of Layer 3 shortcut) do not age out based on the VLAN aging timer. If the routed MAC aging time is modified from the default value, the VLAN aging time is not used. This problem is resolved in Release 12.1(14)E. (CSCdy33647)
- The L3Capture2 diagnostic test might fail during bootup. This problem is resolved in Release 12.1(14)E. (CSCdy30707)
- The following message may display:

  ```
  %LINK-SP-2-NOSOURCE: Source idb not set-Process= "<interrupt level>", ipl= 1,
  pid= 78 -Traceback=
  ```

  This problem is resolved in Release 12.1(14)E. (CSCdy18548)
- The SNMP cefcFRUInserted and cefcFRURemoved notifications are not generated when a GBIC is inserted or removed. This problem is resolved in Release 12.1(14)E. (CSCdy03042)
- When the route for a prefix is advertised by both BGP and IGP and the BGP session goes down, the IGP route for the prefix takes over and LDP allocates and advertises the label for it. When the BGP session comes up, the LDP session withdraws the label after a 5-minute wait. Traffic is dropped until the label is withdrawn. This problem is resolved in Release 12.1(14)E. (CSCdx74321)
- If you enter the **clear ip mroute** command, data corruption occurs in the PIM process and a reload might occur. This problem is resolved in Release 12.1(14)E. (CSCdx72670)
- Access lists might disappear from the running-config file following a reload. This problem is resolved in Release 12.1(14)E. (CSCdx52334)
- A reload might occur following a "%ALIGN-1-FATAL" message. This problem is resolved in Release 12.1(14)E. (CSCdx22902)

- The following error messages are displayed immediately after a reload:

```
%SYS-2-INTSCHED: 'sleep for' at level 3 -Process= "Init", ipl= 3, pid= 2 -Traceback=
6064AA94 60633C04 60FFD1C4 611867AC 6066D1CC 60596134 603D1EB0 603D30BC
603C3110 603D1C20 603BCB30601F2480 601F0460 601F09F0 601F0840 60599A60
```

  The **ip cef** global configuration command and the police settings are class-map configurations and need to have a packet identification mechanism before anything is policed (such as match protocol http). This condition does not occur until the policy map is attached to an interface. This symptom is observed after a reload after it had been configured with the following commands:

```
ip cef
     policy-map test-policy
       class-map test-class
         match protocol http
         police cir 64000 bc 16000 pir 64000 be 16000
         conform-action set-clp-transmit
         exceed-action set-clp-transmit
         violate-action set-clp-transmit
     interface e3/1
       service-policy input test-policy
```

  This problem is resolved in Release 12.1(14)E. (CSCdw20801)

- The Open Shortest Path First (OSPF) designated router might generate router link states but not network link states for a connected network. The OSPF neighbors might come up correctly on all the routers in the network. This problem is resolved in Release 12.1(14)E. (CSCdu08686)
- When multicast support is configured, a spurious memory access or a reload might occur. This problem is resolved in Release 12.1(14)E. (CSCdy85185)
- The **show power** command might incorrectly display a standby Supervisor Engine 2 as a Supervisor Engine 1. This problem is resolved in Release 12.1(14)E. (CSCdy56620)
- Cisco IOS software incorrectly replies to TCP packets that are destined to broadcast/multicast addresses. Replies are sourced from the broadcast/multicast address.

  The problem is applicable to all ports except HTTP (default 80) and HTTPS (default 443) ports.

  With the fix in this DDTS, behavior is changed so that Cisco IOS software will only reply to packets that are destined to broadcast/multicast addresses HTTP (default 80) and HTTPS (default 443) ports. This behavior is further modified by CSCdv30676.

  Although this behavior does not cause any problem for router operation, it may be used for bypassing packet filters (that are configured either in front of or on the router) to reach the services running on TCP (i.e Telnet or SSH) authentication (if configured) still takes place for these services.

  This may be possible if the packet filter allows broadcast/multicast destinations but filter the unicast address of the router.

  A filter that can be bypassed on the affected router may be similar to the following

```
access-list 100 deny ip any host <routers-interface-IP-address>
access-list 100 permit ip any any

interface X/Y
    ip access-group 100 in
```

  This problem is resolved in Release 12.1(14)E. (CSCdy20364)

- When an Internet Group Management Protocol (IGMP) receive message is entered on the incoming interface toward the Route Processor (RP), and a source, group (S,G) R state already exists for a source, the -R flag does not clear. The receiver does not receive traffic for that particular (S,G) entry. This problem is resolved in Release 12.1(14)E. (CSCdx95449)

- Reads and writes to Advanced Technology Attachment (ATA) flash filesystem devices are extremely slow. This problem is resolved in Release 12.1(14)E. (CSCdz27200)
- In rare situations, an MSFC2 might freeze when it can receive control traffic from the supervisor engine, but it cannot send it. This problem is resolved in Release 12.1(14)E. (CSCdy15598)
- The **show interface gigabitethernet output** command incorrectly displays significant deviation between the TXload and RXload parameters. This problem is resolved in Release 12.1(14)E. (CSCdx40459)
- If the length field in the MSDP TLV is less than the minimum MSDP TLV size (3 bytes), memory corruption might occur and cause the system to reload. This problem is resolved in Release 12.1(14)E. (CSCdz25339)
- A Cisco Router that has run out of processor memory may unexpectedly reload due to a bus error at an invalid address if there is an attempt to connect with secure shell (ssh) into a vty port, which fails due to a process creation failure. A SYS-2-CFORKMEM error message appears before the restart. This problem is resolved in Release 12.1(14)E. (CSCdt13023)
- During a PVC discovery test on an ATM port adapter, the MSFC hangs while trying to create a subinterface for the PVC discovery. This problem is resolved in Release 12.1(14)E. (CSCdy71452)
- Following a number of "-SP-" malloc-related error messages, the supervisor engine might run out of memory and reload. This problem is resolved in Release 12.1(13)E1. (CSCdy53239)
- In a redundant Cisco IOS server load balancing (Cisco IOS SLB) configuration, a reload might occur if you enter the **debug ip slb replicate** command or the **debug ip slb all** command. This problem is resolved in Release 12.1(14)E. (CSCin19541)
- When the PBR next hop is not accessible, the new next hop information is not programmed into hardware. This problem is resolved in Release 12.1(14)E. (CSCdy31272)
- A reload might occur after RFSS_server_action messages. This problem is resolved in Release 12.1(14)E. (CSCdy10699)
- When PIM sends an Internet Group Management Protocol (IGMP) receive message on the ingress interface of the MSFC and an (S,G) R state already exists for a source, the -R flag does not clear. The receiver does not receive traffic for that particular (S,G) entry. This problem is resolved in Release 12.1(14)E.
- Auto-Rendezvous Point forwarding may stop working after the state of an interface changes. This symptom is observed on an interface after a route link goes down then comes back up. This problem is resolved in Release 12.1(14)E. (CSCdx89761)
- The **distribute-list 10 in ethernet 10** router configuration command may not be saved under a Virtual Private Network (VPN) routing and forwarding (VRF) instance. This problem is resolved in Release 12.1(14)E. (CSCdz38773)
- A router that is running cell-mode tag switching or Multiprotocol Label Switching (MPLS) on a label controlled ATM (LC-ATM) interface may reload when it receives a more specific prefix for a label mapping or binding than the one that is already allocated. For example, the router may reload when it receives the prefix 10.1.1.0/24 if a binding was already allocated for 10.1.1.1/32 on the basis of the routing entry 10.1.0.0/16. This symptom is observed on an Edge Label Switch Router (ELSR) or Label Switch Controller (LSC). This problem is resolved in Release 12.1(14)E. (CSCdy51183)
- IP connectivity may be lost and a Telnet session to the system may lock up when the **crypto map map-name seq-num ipsec-isakmp** global configuration command is entered. This symptom is observed when a Telnet session is made to a router over a generic routing encapsulation (GRE)-IP Security (IPsec) tunnel and when a new crypto map entry is added to an existing crypto map that is

already applied to the GRE-IPsec tunnel and the associated physical interface. This symptom affects only the GRE-IPsec tunnel and not the IPsec tunnel. This problem is resolved in Release 12.1(14)E. (CSCdy37551)

- HSRP does not validate the destination IP address of received packets. This problem is resolved in Release 12.1(14)E. (CSCdx82139)
- Multiprotocol Label Switching (MPLS) packets entering 802.1Q Ethernet VLAN subinterfaces will not be Cisco express forwarding (CEF) switched. This problem is resolved in Release 12.1(14)E. (CSCdu39979)
- If you replace a **set ip dscp** or **set ip precedence** class map command with a **police** class map command, the class map is deleted. This problem is resolved in Release 12.1(14)E. (CSCdy42355, CSCdy41975)
- With the **ip pim spt-threshold infinity** command configured, if there is an (S,G) entry without its SPT bit set, the (*,G) entry might not be partially Layer 3 switched, which might cause routers not to forward packets on the (S,G) entry. This problem is resolved in Release 12.1(14)E. (CSCdy73168)
- Memory is not released correctly when a port transitions between up and down. This problem is resolved in Release 12.1(14)E. (CSCdy57025)
- After a fatal error, auto-reload fails. This problem is resolved in Release 12.1(14)E. (CSCdy38915)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(14)E, page 224
- Resolved FlexWAN Module Caveats in Release 12.1(14)E, page 224

Open FlexWAN Module Caveats in Release 12.1(14)E

- In a system installed with a FlexWAN and a PA-A3 ATM port adapter, the ATM interface may stay down after you enter a **shutdown** command followed immediately by a **no shutdown** command.

  Workaround: After you enter the **shutdown** command on the interface, wait for 1 minute before entering the **no shutdown** command. This problem is resolved in Release 12.1(20)E. (CSCdy23751, CSCdw65799)

Resolved FlexWAN Module Caveats in Release 12.1(14)E

- After you move multilink members from one FlexWAN module to another, traffic does not pass through the multilink interface. This problem is resolved in Release 12.1(14)E. (CSCdy24019)
- After an OIR, a FlexWAN module may fail to save a crash-information file after a reset if it has a Packet-over-SONET (POS) port adapter with 500 Frame Relay point-to-point DLCIs in Bay 0 and an ATM port adapter with 500 point-to-point operation, administration, and maintenance PVCs in Bay 1. This problem is resolved in Release 12.1(14)E. (CSCdy18458, CSCdy09631)
- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan***slot_number/port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module **crashinfo** file with the **copy cwan***slot_number/port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)

Service Modules Caveats

- Open Service Modules Caveats in Release 12.1(14)E, page 225
- Resolved Service Module Caveats in Release 12.1(14)E, page 225

Open Service Modules Caveats in Release 12.1(14)E

None.

Resolved Service Module Caveats in Release 12.1(14)E

- Do not define VLANs 1002 through 1005 as secure VLANs with the **firewall vlan-group** command. This problem is resolved in Release 12.1(14)E. (CSCdx88498)
- To avoid an MSFC reload, do not enter the **firewall vlan-group** command with VLAN IDs above 4094. This problem is resolved in Release 12.1(14)E. (CSCdy39310)
- To avoid a reload, do not enter the **show firewall module** *module_number* **stat** command while the WS-SVC-FWM-1-K9 Firewall Services Module is resetting. This problem is resolved in Release 12.1(14)E. (CSCdy53164)

OSM Caveats

- Open OSM Caveats in Release 12.1(14)E, page 225
- Resolved OSM Caveats in Release 12.1(14)E, page 225

Open OSM Caveats in Release 12.1(14)E

None.

Resolved OSM Caveats in Release 12.1(14)E

- In a system with a channelized DS3 OSM installed and more than 10,000 IP routes present, the following error message may be displayed for the channelized DS3 OSM:

  ```
  FIB-3-FIBDISABLE: Fatal error, slot/cpu 4/0: no memory
  ```

  This problem is resolved in Release 12.1(14)E. (CSCdy19072, CSCdy40632)
- With Ethernet over MPLS, a problem may occur when the label switched path (LSP) for an Ethernet over MPLS VC is changed and a new tunnel label for the new LSP is used. Instead of sending the frame with the new tunnel label, the frame is sent with the old tunnel label. This problem is resolved in Release 12.1(14)E. (CSCdy34983)
- In a system with a large number of Frame Relay subinterfaces configured, some subinterfaces will not be functional after the system switches over from the active route processor to the redundant route processor. This problem is resolved in Release 12.1(14)E. (CSCdy26531)
- If multiple OC-12-ATM OSMs with large configurations are installed in a system, you may not be able to boot the OC-12-ATM OSMs simultaneously. This problem is resolved in Release 12.1(14)E. (CSCdy21621, CSCdy14468)
- Hierarchical traffic shaping is not supported for Frame Relay on the channelized OSMs. This problem is resolved in Release12.1(14)E. (CSCdx75683)

- Following a reload, it is safe to ignore this message from OSM-2OC12-POS-MM, OSM-2OC12-POS-SI, or OSM-2OC12-POS-SL modules in a fully loaded chassis:

```
%SM-SP-4-BADEVENT: Event 'dnld_completed' is invalid for the current state
'online': scp_dnld_module 4
```

  This problem is resolved in Release 12.1(14)E. (CSCdw10533)

Release 12.1(13)E and Rebuilds

Note All caveats resolved in Release 12.1(11b)EX are resolved in Release 12.1(13)E. Refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12111bex/ol_2720.htm#282050

- General Caveats, page 226
- FlexWAN Module Caveats, page 252
- Service Modules Caveats, page 255
- OSM Caveats, page 257

General Caveats

- Open General Caveats in Release 12.1(13)E17, page 227
- Resolved General Caveats in Release 12.1(13)E17, page 227
- Resolved General Caveats in Release 12.1(13)E16, page 227
- Resolved General Caveats in Release 12.1(13)E15, page 228
- Resolved General Caveats in Release 12.1(13)E14, page 229
- Resolved General Caveats in Release 12.1(13)E13, page 232
- Resolved General Caveats in Release 12.1(13)E12, page 233
- Resolved General Caveats in Release 12.1(13)E11, page 235
- Resolved General Caveats in Release 12.1(13)E10, page 235
- Resolved General Caveats in Release 12.1(13)E9, page 237
- Resolved General Caveats in Release 12.1(13)E8, page 237
- Resolved General Caveats in Release 12.1(13)E7, page 238
- Resolved General Caveats in Release 12.1(13)E6, page 240
- Resolved General Caveats in Release 12.1(13)E5, page 241
- Resolved General Caveats in Release 12.1(13)E4, page 243
- Resolved General Caveats in Release 12.1(13)E3, page 244
- Resolved General Caveats in Release 12.1(13)E1, page 247
- Resolved General Caveats in Release 12.1(13)E, page 249

Open General Caveats in Release 12.1(13)E17

- If you replace a **set ip dscp** or **set ip precedence** class map command with a **police** class map command, the class map is deleted. This problem is resolved in Release 12.1(14)E. (CSCdy42355, CSCdy41975)

Resolved General Caveats in Release 12.1(13)E17

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

  This problem is resolved in Release 12.1(13)E17. (CSCei61732)
- Receipt of a Border Gateway Protocol (BGP) Autonomous System (AS) path with a length that is equal to or greater than 255 might reset the BGP session. This problem is resolved in Release 12.1(13)E17. (CSCeh13489)

Resolved General Caveats in Release 12.1(13)E16

- A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

  Cisco has made free software available to address this problem.

  For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

  This problem is resolved in Release 12.1(13)E16. (CSCee67450)
- A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

  Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

  The Advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

  This problem is resolved in Release 12.1(13)E16. (CSCef46191)

- A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

  This problem is resolved in Release 12.1(13)E16. (CSCed78149)

Resolved General Caveats in Release 12.1(13)E15

- A reload might occur when traffic enters a port configured with the **switchport protocol ip auto** command. This problem is resolved in Release 12.1(13)E15. (CSCin77984)
- With the Response Time Reporter (RTR) feature configured, spurious accesses might occur. This problem is resolved in Release 12.1(13)E15. (CSCdy56859)
- When multicast support is configured, a spurious memory access or a reload might occur. This problem is resolved in Release 12.1(13)E15. (CSCdy85185)
- If there are more than 50 files on the flash card, access from CiscoView Device Manager (CVDM) might cause a reload. This problem is resolved in Release 12.1(13)E15. (CSCef07965)
- While traffic is flowing, CPU utilization might increase to a very high level if you reconfigure an EtherChannel from Layer 3 to Layer 2 and configure a Layer 3 VLAN interface for the EtherChannel. This problem is resolved in Release 12.1(13)E15. (CSCee41100)
- Occasionally, these modules might lose the ability to communicate over the Ethernet Out of Band Channel (EOBC) and reset:
  - WS-X6416-GBIC
  - WS-X6348-RJ-45
  - WS-X6148-RJ-45
  - WS-X6348-RJ-21
  - WS-X6148-RJ-21
  - WS-X6316-GE-TX

  - WS-X6324-100FX
  - WS-X6416-GE-MT
  - WS-X6024-10FL-MT

  This problem is resolved in Release 12.1(13)E15. (CSCef23843)

- Traffic loss might occur on fabric-enabled modules when there are frequent OIRs. This problem is resolved in Release 12.1(13)E15. (CSCee44496, CSCee48403, CSCee78766)
- OSPF area border routers (ABRs) might continue to generate summary link-state advertisements (LSAs) for obsolete nonbackbone intra-area routes. This problem is resolved in Release 12.1(13)E15. (CSCee36622)
- Traffic through a port-channel interface that has a Cisco IOS ACL configured might be dropped or switched in software after a reload or after switchover to a redundant supervisor engine or after you enter **shutdown** and **no shutdown** interface commands on a member port. This problem is resolved in Release 12.1(13)E15. (CSCee21772)
- With a switch fabric module (SFM), some modules might stop egressing traffic. This problem is resolved in Release 12.1(13)E15. (CSCee08015)
- In releases where caveat CSCdz27200 is resolved, files copied to an Advanced Technology Attachment (ATA) disk might be corrupt. This problem is resolved in Release 12.1(13)E15. (CSCed44319)
- Under heavy traffic conditions, online insertion and removal (OIR) of a switch fabric module or OIR of a nonfabric-enabled module might cause OSMs to stop forwarding traffic. This problem is resolved in Release 12.1(13)E15. (CSCec49269)
- After you remove a Cisco IOS ACL from an interface, the packets continue to be passed or dropped as they would with the Cisco IOS ACL still attached. This problem is resolved in Release 12.1(13)E15. (CSCec43666)
- With other fabric-enabled modules installed, a WS-X6816-GBIC module does not come online after a hot insert or software reset. This problem is resolved in Release 12.1(13)E15. (CSCec27072)
- OSPF might set the partial database flag without a partial shortest path first (SPF) ever happening when a link-state advertisement (LSA) update received from a neighbor has a different mask than that in previous LSA updates, which might prevent the LSA from being deleted from the OSPF database. This problem is resolved in Release 12.1(13)E15. (CSCdz82284)
- If SrBuildSnmpMessage fails and the Simple Network Management Protocol (SNMP) performs an SNMP memcpy operation on the invalidated memory, memory corruption might cause a reload. This problem is resolved in Release 12.1(13)E15. (CSCdt12634)

Resolved General Caveats in Release 12.1(13)E14

- With certain configurations, a reload might occur when you enter the **show cdp entry * protocol** command. This problem is resolved in Release 12.1(13)E14. (CSCed40563)
- With fall-back bridging configured, ARP fails after a switchover to the redundant supervisor engine. This problem is resolved in Release 12.1(13)E14. (CSCed61632)
- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the

sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

This problem is resolved in Release 12.1(13)E14. (CSCed93836, CSCdz84583)

- With a loopback cable from a trunk port connected to a WAN port acting as an MPLS/VPN interface, an unresolved default route causes the PFC to send packets to the MSFC for ARP resolution, which interferes with hardware switching of the packets exiting the loopback port. This problem is resolved in Release 12.1(13)E14. (CSCed64844)
- A reload might occur after you shut down a Gigabit Ethernet interface. This problem is resolved in Release 12.1(13)E14. (CSCed58452)
- TCP FIN and RST packets might be dropped, which causes a 3 to 4 second delay in retrieving web content, if a hardware-switched TCP connection carrying more than 1,000 packets per second is load balanced through IOS Firewall Load Balancing or Cisco IOS server load balancing. This problem is resolved in Release 12.1(13)E14. (CSCed38956)
- With a PFC2 and with EtherChannels configured to include interfaces on different DFC-equipped switching modules, ARP traffic from a WS-X6066-SLB-APC Content Switching Module (CSM) that is running software version 3.2(2) and earlier might not be forwarded correctly. This problem is resolved in Release 12.1(13)E14. (CSCed35745)
- These switching modules might reset when a link contiguously goes from down to up to down within 300 milliseconds.
  - WS-6248-RJ45
  - WS-6248-TEL
  - WS-6348-RJ45
  - WS-6348-RJ21
  - WS-6148-RJ45
  - WS-6148-RJ21
  - WS-6348-100FX

  This problem is resolved in Release 12.1(13)E14. (CSCed17719)
- In rare situations, the MTU size on a WS-X6548-RJ-45 switching module might not be programmed correctly in hardware. This problem is resolved in Release 12.1(13)E14. (CSCed90989, CSCed10458)
- It is possible for an invalid **override-mac-address** command to be accepted at boot time if you use a configuration file from one system on another. This problem is resolved in Release 12.1(13)E14. (CSCeb83558)
- The **show power** command might incorrectly display a standby Supervisor Engine 2 as a Supervisor Engine 1. This problem is resolved in Release 12.1(13)E14. (CSCdy56620)

- Cisco IOS software incorrectly replies to TCP packets that are destined to broadcast/multicast addresses. Replies are sourced from the broadcast/multicast address.

  The problem is applicable to all ports except HTTP (default 80) and HTTPS (default 443) ports.

  With the fix in this DDTS, behavior is changed so that Cisco IOS software will only reply to packets that are destined to broadcast/multicast addresses HTTP (default 80) and HTTPS (default 443) ports. This behavior is further modified by CSCdv30676.

  Although this behavior does not cause any problem for router operation, it may be used for bypassing packet filters (that are configured either in front of or on the router) to reach the services running on TCP (i.e Telnet or SSH) authentication (if configured) still takes place for these services.

  This may be possible if the packet filter allows broadcast/multicast destinations but filter the unicast address of the router.

  A filter that can be bypassed on the affected router may be similar to the following

  ```
  access-list 100 deny ip any host <routers-interface-IP-address>
  access-list 100 permit ip any any

  interface X/Y
      ip access-group 100 in
  ```

  This problem is resolved in Release 12.1(13)E14. (CSCdy20364)

- When an Internet Group Management Protocol (IGMP) receive message is entered on the incoming interface toward the Route Processor (RP), and a source, group (S,G) R state already exists for a source, the -R flag does not clear. The receiver does not receive traffic for that particular (S,G) entry. This problem is resolved in Release 12.1(13)E14. (CSCdx95449)
- The **squeeze** command might cause high CPU utilization for several minutes. This problem is resolved in Release 12.1(13)E14. (CSCdz60750)
- A new vulnerability in the OpenSSL implementation for SSL has been announced on March 17, 2004.

  An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack. There are workarounds available to mitigate the effects of this vulnerability on Cisco products in the workaround section of this advisory. Cisco is providing fixed software, and recommends that customers upgrade to it when it is available.

  This advisory will be posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml

  This problem is resolved in Release 12.1(13)E14. (CSCee00041)

- Many memory allocation failure (MALLOCFAIL) messages might occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
  Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  This problem is resolved in Release 12.1(13)E14. (CSCdz32659)

- Receiving CDP packets with a host name that is 256 or more characters long might cause a memory leak in the CDP process. This problem is resolved in Release 12.1(13)E14. (CSCin67568)
- Following “cmd failed” messages for ATM configuration commands, an ATM interface might remain administratively down. This problem is resolved in Release 12.1(13)E14. (CSCin40163)

- After Cisco IOS ACLs have been updated dynamically or after responding dynamically to an IDS signature, a reload might occur following attempts to access a low memory address. This problem is resolved in Release 12.1(13)E14. (CSCed35253)
- A reload might follow receipt of a corrupt CPD packet. This problem is resolved in Release 12.1(13)E14. (CSCec25430)
- Occasionally, multicast traffic that should be completely Layer 3-switched is partially Layer 3-switched, which causes multicast packets to be dropped when the ACL TCAM is full. This problem is resolved in Release 12.1(13)E14. (CSCin63402)
- High-volume SNMP traffic might cause a reload. This problem is resolved in Release 12.1(13)E14. (CSCed79519)
- A VLAN with no active ports might not be shut down correctly. This problem is resolved in Release 12.1(13)E14. (CSCed47381)
- Occasionally after a reload, the IDPROM is not read correctly on a WS-X6548-RJ-45 switching module that is equipped with a DFC, which holds the module in the "other" state. This problem is resolved in Release 12.1(13)E14. (CSCed04988)
- The following message might be followed by a reload:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0xX, ra=0xXXXXXXXX, sp=0xXXXXXXXX
  ```

  This problem is resolved in Release 12.1(13)E14. (CSCeb48670)
- Routing Information Protocol version 2 (RIPv2) routes get stuck in the routing table, even if the next hop interface is down. This problem is resolved in Release 12.(13)E14. (CSCea47597)
- When TTL propagation has been turned off by entering the **tag-switching ip propagate-ttl** command, MPLS TTLs are still copied to IP packets. This problem is resolved in Release 12.1(13)E14. (CSCdy47341)
- With both static and dynamic Port Address Translation (PAT) configured and if the **ip nat pool** *inside_pool_name* command has been entered for only one IP address, the IP addresses that are used for overloading might be used as one-to-one translations. This problem is resolved in Release 12.1(13)E14. (CSCdx19396)

Resolved General Caveats in Release 12.1(13)E13

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

This problem is resolved in Release 12.1(13)E13. (CSCed27956, CSCed38527)

- Malfunctioning PIM, MLSM, or mwheel processes might cause "CPUHOG" and "WATCHDOG" messages and reloads. This problem is resolved in Release 12.1(13)E13. (CSCed12393)
- When fragmenting MPLS traffic, a reload might occur after display of a "SYS-2-GETBUF" message. This problem is resolved in Release 12.1(13)E13. (CSCeb16876)
- The **show disk0:** command does not work. This problem is resolved in Release 12.1(13)E13. (CSCin64119)
- Traffic might flow in only one direction after assigning a LAN port to a different VLAN. This problem is resolved in Release 12.1(13)E13. (CSCed20566)
- To avoid dropping into ROMMON, do not insert a WS-X6816-GBIC that does not have a DFC installed. This problem is resolved in Release 12.1(13)E13. (CSCed14506)
- Occasionally, the nvram:/startup-config file cannot be read. This problem is resolved in Release 12.1(13)E13. (CSCed06462)
- Directly connected multicast enabled subnets might not be programmed correctly into the PFC. This problem is resolved in Release 12.1(13)E13. (CSCed00394)
- With a complex Spanning Tree topology (for example, a high number of blocked ports in the same VLAN), if an inferior BPDU is received at approximately the same time that the message age timer expires, STP might send out BPDUs with obsolete information (for example, the previous root ID) for the duration of the maximum age timer, which can delay STP convergence. This problem is resolved in Release 12.1(13)E13. (CSCea68988)
- A reload might occur if you use SNMP to disable the EOBC0/0 interface through ifAdminStatus. This problem is resolved in Release 12.1(13)E13. (CSCea53440)
- In releases where caveat CSCdz27200 is resolved, a reload might occur when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) flash card (for example, disk0). For example, this situation may occur when you enter the **show** *command_name* **| tee /append** *url* privileged EXEC command. This problem is resolved in Release 12.1(13)E13. (CSCin57765)
- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

  This problem is resolved in Release 12.1(13)E13. (CSCed28873)

Resolved General Caveats in Release 12.1(13)E12

- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been

developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

This problem is resolved in Release 12.1(13)E12. (CSCea46342, CSCdx76632, CSCin56408, CSCdx40184, CSCec76776)

- When there is insufficient memory, crash information is not generated after a Supervisor Engine reload. This problem is resolved in Release 12.1(13)E12. (CSCeb51785)
- The system resets when the AAA protocol is configured for accounting. This problem is resolved in Release 12.1(13)E12. (CSCeb42177)
- With Multicast Source Discovery Protocol (MSDP) configured, a reload might occur if you enter the **show ip msdp peer** *ip_address* **advertised-SAs** command. This problem is resolved in Release 12.1(13)E12. (CSCec23559)
- An IGMP packet flood might cause a reload. This problem is resolved in Release 12.1(13)E12. (CSCec39132)
- A reload might occur when a TCP session is cleared. This problem is resolved in Release 12.1(13)E12. (CSCdw76948)
- With the Protocol Independent Multicast (PIM) Dense-Mode State Refresh feature enabled, a reload might occur if the group mode changes from PIM dense mode to PIM sparse or bidirectional mode. This problem is resolved in Release 12.1(13)E12. (CSCea09302)
- With Layer 2 protocol tunneling configured, VTP traffic might be incorrectly dropped by IEEE 802.1Q tunnels. This problem is resolved in Release 12.1(13)E12. (CSCec11165)
- OIR of a fabric-enabled switching module might cause a reload. This problem is resolved in Release 12.1(13)E12. (CSCec12236)
- A reload might occur if you modify a policy map that is attached to an interface. This problem is resolved in Release 12.1(13)E12. (CSCec15119)
- With EoMPLS configured, a reload might occur if you configure a different access VLAN on the CE-facing port. This problem is resolved in Release 12.1(13)E12. (CSCec23787)
- A FIB-related memory leak might occur. This problem is resolved in Release 12.1(13)E12. (CSCec43573)
- With VLAN aging configured, the routed MAC (RM) bit might be set on the Layer 2 entries for routed traffic, which causes the entries to be purged every 5 minutes. One packet might be flooded and relearned for each purged entry. This problem is resolved in Release 12.1(13)E12. (CSCec43605)
- With a large number of static multicast entries configured (approximately 8,000), some entries might not propagate to DFCs. This problem is resolved in Release 12.1(13)E12. (CSCec50577)
- L3-PS-DRVR messages are seen every 12 to 16 seconds. This problem is resolved in Release 12.1(13)E12. (CSCec63833)
- For BGP routes learned through a WAN interface, if the BGP neighbor goes down, the default route adjacency does not change if the default route learned through BGP had a better metric than a static route configured locally. This problem is resolved in Release 12.1(13)E12. (CSCec41005)

Resolved General Caveats in Release 12.1(13)E11

- The **show mac-address-table** command might incorrectly display "<drop>" instead of "flood to vlan" for a MAC address. This is a cosmetic error. This problem is resolved in Release 12.1(13)E11. (CSCdz83191)
- Incorrect traffic loss occurs if you enter a **shutdown** command and then a **no shutdown** command on a Layer 3 VLAN interface that has HSRP configured. This problem is resolved in Release 12.1(13)E11. (CSCec26522)
- The WS-X6348-RJ-45, WS-X6248-RJ-45, WS-X6248-TEL, and WS-X6348-RJ-21V modules might randomly reset. This problem is resolved in Release 12.1(13)E11. (CSCeb35612)

Resolved General Caveats in Release 12.1(13)E10

- The **scheduler allocate command** process-time default value is too small (200 microseconds, changed to 800 microseconds with this fix). The **no scheduler allocate** command does not return the configuration to default values. These problems are resolved in Release 12.1(13)E10. (CSCeb75803)
- There might be OSPF neighbor drops and HSRP flaps when QoS is enabled on a Supervisor Engine 1 and MSFC2. This problem is resolved in Release 12.1(13)E10. (CSCeb55271)
- Routing protocols do not work on EtherChannels that are reconfigured from Layer 2 to Layer 3. This problem is resolved in Release 12.1(13)E10. (CSCeb60132)
- An IEEE 802.Q trunking Gigabit EtherChannel formed with interfaces on different DFC-equipped switching modules might drop some traffic that is Layer 3 switched in hardware or that is routed in software. This problem is resolved in Release 12.1(13)E10. (CSCeb05464)
- With the **ip pim spt-threshold infinity** command configured, if there is an (S,G) entry without its SPT bit set, the (*,G) entry might not be partially Layer 3 switched, which might cause routers not to forward packets on the (S,G) entry. This problem is resolved in Release 12.1(13)E10. (CSCdy73168)
- When a Cisco IOS server load balancing (Cisco IOS SLB) virtual server is configured for RADIUS load balancing with the **msid-cisco** keyword, then Accounting-Start RADIUS requests from a Home Agent may not be load-balanced to the same real server as the Access-Request. This problem is resolved in Release 12.1(13)E10. (CSCeb00351)
- On WS-X6548-GE-TX and WS-X6548V-GE-TX modules, CEF-switched Ethernet egress packets that are less than 64-bytes long are not padded correctly. This problem is resolved in Release 12.1(13)E10. (CSCeb47640)
- After a fatal error, auto-reload fails. This problem is resolved in Release 12.1(13)E10. (CSCdy38915)
- Memory is not released correctly when a port transitions between up and down. This problem is resolved in Release 12.1(13)E10. (CSCeb82767, CSCdy57025)
- A redundant supervisor engine might not reload if you enter the reload command on the redundant supervisor engine's console or physically remove and reinsert the redundant supervisor engine. This problem is resolved in Release 12.1(13)E10. (CSCea66858)
- When not configured with a redundant power supply, continuous reloads might happen if the output from the single power supply is momentarily unstable, which causes this message to be displayed:

  ```
  "%C6KPWR-2-INSUFFICIENTPOWER: Powering down all linecards as there is not enough power
  to operate all critical cards"
  ```

  This problem is resolved in Release 12.1(13)E10. (CSCea82777)

- If you replace a WS-X6148-GE-TX or WS-X6148V-GE-TX switching module with a WS-X6548-GE-TX or WS-X6548V-GE-TX switching module, any **switchport** commands configured on the WS-X6148-GE-TX or WS-X6148V-GE-TX switching module do not work on the WS-X6548-GE-TX or WS-X6548V-GE-TX switching module. This problem is resolved in Release 12.1(13)E10. (CSCea89432)
- Deny ACEs that do not specify any Layer 4 ports incorrectly do not deny fragmented packets. This problem is resolved in Release 12.1(13)E10. (CSCeb04343)
- With IGMP snooping configured on a VLAN, but with PIM not enabled on the Layer 3 VLAN interface, PIM register and register-stop packets are routed to the interface on which they are received causing additional load on the network and MSFC. This problem is resolved in Release 12.1(13)E10. (CSCeb12540)
- The **show mls qos** command might incorrectly show support for egress QoS. This problem is resolved in Release 12.1(13)E10. (CSCeb29483)
- With a Supervisor Engine 2, the IOS ARP and adjacency entries for the next-hop IP address configured for a static route might not be created. This problem is resolved in Release 12.1(13)E10. (CSCeb38062)
- With RPR redundancy configured, the MSFC and OSMs might incorrectly reload. This problem is resolved in Release 12.1(13)E10. (CSCeb49134)
- The CEF entries for traffic from a directly connected Layer 3 address are removed and recreated randomly, which causes Unicast traffic loss for the affected entries. This problem is resolved in Release 12.1(13)E10. (CSCeb53542)
- Incorrect VTP pruning might occur if you delete or rename VLANs in VLAN database mode. This problem is resolved in Release 12.1(13)E10. (CSCeb60262)
- Supervisor Engine 1 does not have RP-SP inband channel communication monitoring. This problem is resolved in Release 12.1(13)E10. (CSCeb46610)
- Memory usage when handling route flaps is not optimal, which causes the route-flap handling process to hold memory longer than necessary and which can cause out-of-memory conditions when routes flap continuously. This problem is resolved in Release 12.1(13)E10. (CSCeb57465)
- When the multicast traffic level exceeds the Layer 3 hardware switching capacity, the excess multicast traffic might be dropped instead of being routed in software on the MSFC. This problem is resolved in Release 12.1(13)E10. (CSCeb62692)
- If you enter the **shutdown** command and then the **no shutdown** command on an interface that is handling a high volume of Layer 3 hardware switched multicast traffic, some of the multicast traffic is routed in software on the MSFC instead of being Layer 3 switched in hardware when the interface comes back up. This problem is resolved in Release 12.1(13)E10. (CSCeb67996)
- With QoS and Cisco IOS server load balancing (Cisco IOS SLB) configured on a Supervisor Engine 1, a VACL configured to filter multicast traffic on one VLAN might incorrectly be applied to multicast traffic on other VLANs. This problem is resolved in Release 12.1(13)E10. (CSCeb69582)
- If you configure the **mac-address-table aging-time** command with a nonzero value, a static MAC address for traffic that egresses through a DFC-equipped card might change to a dynamic MAC address. This problem is resolved in Release 12.1(13)E10. (CSCeb72014)
- With PBR configured on an interface, if the link goes down or if you enter a clear arp command, traffic that should be Layer 3 switched in hardware might be routed in software on the MSFC. This problem is resolved in Release 12.1(13)E10. (CSCeb78050)
- Multicast traffic that should be Layer 3 switched in hardware might be dropped or routed in software on the MSFC. This problem is resolved in Release 12.1(13)E10. (CSCeb80373)

- Some traffic that ingresses through one DFC-equipped module and egresses through another DFC-equipped module might be dropped. This problem is resolved in Release 12.1(13)E10. (CSCeb83650)
- With CBAC and RPR+ redundancy configured, all TCP and UPD sessions fail after a switchover to the redundant supervisor engine. This problem is resolved in Release 12.1(13)E10. (CSCeb87003)
- Following a reload, a Supervisor Engine 2 with the **no mls qos channel-consistency** command configured might display an erroneous "qos-card type" mismatch message for an EtherChannel and incorrectly refuse to include some of the ports in the EtherChannel. This problem is resolved in Release 12.1(13)E10. (CSCec00966)
- With a Supervisor Engine 2, if you enter a **clear mac-address-table dynamic** command, traffic between DFC-equipped and nonDFC-equipped modules might be dropped for approximately 10 minutes. This problem is resolved in Release 12.1(13)E10.
- After an RPR+ switchover, if you have configured the **mls ip directed broadcast** command, all broadcast traffic is sent to the MSFC to be processed in software. This problem is resolved in Release 12.1(13)E10. (CSCec07319)
- A redundant supervisor engine might incorrectly run out of memory while in the standby state and be unable to support a switchover. This problem is resolved in Release 12.1(13)E10. (CSCec08966)
- With port security enabled, a memory leak might occur. This problem is resolved in Release 12.1(13)E10. (CSCec14266)

Resolved General Caveats in Release 12.1(13)E9

- When you configure interface speed and duplex mode, you must configure speed before you can configure the duplex mode. The speed and duplex mode configuration is stored in the configuration file in reverse order, which causes duplex mode configuration failure if you paste in a configuration file. This problem is resolved in Release 12.1(13)E9. (CSCea93829)
- The definitions of some MIB objects are incorrectly of type Counter32 instead of type Gauge32. This problem is resolved in Release 12.1(13)E9. (CSCdz65045)
- Environmental polling is invalid on a redundant supervisor engine. This problem is resolved in Release 12.1(13)E9. (CSCdy64272)
- If you enter a **show interface etherchannel** command or a **show interface etherchannel module** command for an EtherChannel with ports on a module that is no longer installed, the MSFC might reload or there might be a switchover to a redundant supervisor engine. This problem is resolved in Release 12.1(13)E9. (CSCeb53215)
- With a redundant supervisor engine installed, the configuration of EtherChannels that are reconfigured from Layer 2 to Layer 3 is not synchronized to the redundant supervisor engine. This problem is resolved in Release 12.1(13)E9. (CSCeb56353)
- With a redundant supervisor engine installed, if you enter the **switchport** or **no switchport** command in interface range mode, the configuration on the redundant supervisor engine for the range of interfaces might not be synchronized. This problem is resolved in Release 12.1(13)E9. (CSCea23123)

Resolved General Caveats in Release 12.1(13)E8

- A memory leak might occur with Layer 2 aging and EtherChannels that include ports on different DFC-equipped modules configured. This problem is resolved in Release 12.1(13)E8. (CSCeb48732)

Resolved General Caveats in Release 12.1(13)E7

- A manually summarized entry might remain in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table after manual summarization is disabled. This problem is resolved in Release 12.1(13)E7. (CSCdx83729)
- Reads and writes to Advanced Technology Attachment (ATA) flash filesystem devices are extremely slow. This problem is resolved in Release 12.1(13)E7. (CSCdz27200)
- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

  This problem is resolved in Release 12.1(13)E7. (CSCdz71127)
- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

  This problem is resolved in Release 12.1(13)E7. (CSCea02355)
- When EtherChannel is configured, all traffic is flooded to all the ports in the VLAN every 11 minutes. This traffic storm lasts approximately 1.5 seconds and also affects service cards with internal EtherChannel, such as the Content Switching Module (CSM) and Content Services Gateway (CSG). This problem is resolved in Release 12.1(13)E7. CSCea43688)
- Incorrect flooding might occur in a 13-slot chassis with DFCs. This problem is resolved in Release 12.1(13)E7. (CSCeb11577)
- ICMP ping tests fail across a EtherChannel when the “src-dst-port” port-channel load-balance algorithm is used. This problem is resolved in Release 12.1(13)E7. (CSCea42504)
- When you add a /31 netmask route, the new netmask does not overwrite an existing /32 CEF entry. This problem is resolved in Release 12.1(13)E7. A facility has been provided to periodically validate prefixes derived from adjacencies in the FIB against prefixes originating from the RIB. To enable the validation, you must enter the **ip cef table adjacency-prefix validate** global configuration command. (CSCea53765)
- Multicast traffic is process switched after OIR. This problem is resolved in Release 12.1(13)E7. (CSCea80221)
- A system running Cisco IOS 12.1(13)E does not allow a secure MAC address to be removed or reused on a Layer 2 port. This problem is resolved in Release 12.1(13)E7. (CSCea48243)

- In a topology that uses VLAN interfaces for intermediate router connections, PIM register and PIM register stop messages might loop between the intermediate routers until the TTL count expires. This problem is resolved in Release 12.1(13)E7. (CSCea82353)
- With IP inspection configured, a reload might occur following an "%ALIGN-1-FATAL" message. This problem is resolved in Release 12.1(13)E7. (CSCea51320)
- The switch might drop into ROMMON mode after reload. This problem is resolved in Release 12.1(13)E7. (CSCea88910)
- Invalid 64-bit counter values instead of zero values may be returned for IF-MIB Layer 2 VLANs. This problem is resolved in Release 12.1(13)E7. (CSCea59775)
- If a crash information file is written to an ATA Flash PC card, the file on the ATA Flash PC card may be corrupt and unusable. This problem is resolved in Release 12.1(13)E7. (CSCdz81035)
- If the copy operation of an image file to a PC Flash card is interrupted by a system reload or a power failure, the image file might be corrupted. If this image is later copied or used to boot the system, the copy or boot process may fail and display a "sector read failed" error message. This problem is resolved in Release 12.1(13)E7. (CSCdz54387)
- Multicast shortcuts take a long time to install during dense mode fallback, which causes latency in hardware switching. This problem is resolved in Release 12.1(13)E7. (CSCeb14435)
- When you enter a **shutdown** command followed by a **no shutdown** command, or enter a **clear ip mroute** command, the scan timer may not restart and multicast route entries may not be hardware switched. This problem is resolved in Release 12.1(13)E7. (CSCea05404)
- Multicast entries may become inconsistent when configuration changes are made, such as modifying an interface's IP address. The multicast entries are programmed in the hardware, but the software does not reflect the hardware state. This problem is resolved in Release 12.1(13)E7. (CSCea71130)
- User-configured static multicast MAC entries are not processed correctly. When the system first boots, the interface state does not show up/up, and the interface does not get added to the Layer 2 table. Consequently, traffic is not received by the port. This problem is resolved in Release 12.1(13)E7. (CSCea72405)
- On a system with a Supervisor Engine 2, a MSFC 2 and a DFC, when the DFC card is reset, traffic is software switched for those ports that have HSRP enabled. This problem is resolved in Release 12.1(13)E7. (CSCea89099)
- A default route learned through a routing protocol might be either missing or incomplete. This problem is resolved in Release 12.1(13)E7. (CSCeb18552)
- If you enter a **show cdp neighbor** command on a switch connected to another switch with a port channel, the command output may show the same local interface for all member ports in the channel. This problem is resolved in Release 12.1(13)E7. (CSCea15655)
- When using stateful Cisco IOS server load balancing (Cisco IOS SLB) and with the **standby preempt** command configured on some interfaces, a switchover to the redundant supervisor engine might cause high CPU utilization. This problem is resolved in Release 12.1(13)E7. (CSCea54756)
- When the maximum number of RLB sticky subscribers for a real server (SSG1) are exceeded, the RLB does not pass AcctStop packets (from GGSN) to SSG1 for the existing host objects, but to the next SSG in the round-robin pool. The SSG proxies the AcctStop packets to the AAA server, which then closes the corresponding RADIUS sessions. This situation leads to stale host objects on the first SSG. This problem is resolved in Release 12.1(13)E7. (CSCeb09340)
- A reload might occur if you configure an IP address that is a duplicate of an IP address configured on a redistributed BGP peer. This problem is resolved in Release 12.1(13)E7. (CSCdz30644)

- After the link to the PBR next hop is lost, the new next hop information is not programmed into hardware immediately. This problem is resolved in Release 12.1(13)E7. (CSCdy28888)
- Hardware-supported ACLs without any ACEs do not implicitly deny all traffic. This problem is resolved in Release 12.1(13)E7. (CSCea17192)
- A system with an MSFC2 may encounter a bus error if the percent character is used in a VTP password, a VTP domain, or a VTP VLAN name. This problem is resolved in Release 12.1(13)E7. (CSCea82238)
- With the fastest aging time configured and the highest flow creation rates configured, the statistics exported by NetFlow data export are not accurate. The inaccuracy is reduced in Release 12.1(13)E7. (CSCea72771)

Resolved General Caveats in Release 12.1(13)E6

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.1(13)E6. (CSCdu53656)
- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.1(13)E6. (CSCea28131)
- The **show EOBC** command shows a very large retry count when there is a lot of traffic in the Ethernet Out-of-Band channel (EOBC) for a long period of time. This problem is resolved in Release 12.1(13)E6. (CSCea46236)
- When the following conditions occur, some static multicast MAC entries may not get installed in the Layer 2 hardware table:
  - During system load
  - During a system reload
  - During a switchover to the redundant system

  This problem is resolved in Release 12.1(13)E6. (CSCuk37312)
- If a (*,G) shortcut is established as a complete shortcut, and then needs to change to a partial shortcut, the software fails to change the shortcut to a partial shortcut. This problem is resolved in Release 12.1(13)E6. (CSCea66943)

- If you configure Cisco IOS SLB while creating RTR entries using SNMP, the system may generate traceback messages similar to the following:

```
Feb 16 15:27:08.846: %IDMGR-3-INVALID_ID: bad id in id_to_ptr
-Traceback= 413DD97C 405C4C08 405CB12C 40E387E8 40E34DF0 401DAD1C 401DAD08
Feb 16 15:28:08.846: %IDMGR-3-INVALID_ID: bad id in id_to_ptr
-Traceback= 413DD97C 405C4C08 405CB12C 40E387E8 40E34DF0 401DAD1C 401DAD08
```

  This problem is resolved in Release 12.1(13)E6. (CSCea21064)

- When you run the RADIUS load balancing (RLB) feature of IOS server load balancing in a redundant configuration, the standby RLB switch may reload. This problem occurs only if stateful replication of the RADIUS username sticky database is used. This problem is resolved in Release 12.1(13)E6. (CSCea61966)

Resolved General Caveats in Release 12.1(13)E5

- The “do not learn” bit of an active VLAN can incorrectly become set, which prevents any more dynamic CAM entries from being learned for that VLAN and floods all unicast traffic in that VLAN. This problem is resolved in Release 12.(13)E5. (CSCea45950)
- The following OSM ports do not support multicast traffic:
  - OC-3 POS OSM ports 2 through 8
  - OC-12 POS OSM ports 2 through 4
  - OC-12 ATM OSM port 2

  This problem is resolved in Release 12.1(13)E5. (CSCea34141)
- When some multicast RPF interfaces are tunnel interfaces, a Supervisor Engine 1 with an MSFC1 might reload when the routing table changes frequently. This problem is resolved in Release 12.1(13)E5. (CSCea50623)
- If MMLS is not synchronized between the MSFC and the supervisor engine when you enter a **clear ip mr *** command or a **clear ip mroute** *group_address* command, the MMLS entry on the supervisor engine might not be cleared. This problem is resolved in Release 12.1(13)E5. (CSCdy51453)
- In an intermediate router where (*,G) and (S,G) traffic is RPF multicast fast dropped and the (*,G) traffic and the (S,G) traffic have different RPF interfaces, when an RPF change happens for the (S,G) entries, the intermediate router deletes the (S,G) entry but does not delete the (*,G) entry, which causes the multicast traffic to use (*,G) entry in HW and get dropped as non-RPF traffic. This problem is resolved in Release 12.1(13)E5. (CSCea60918)
- A reload might occur when you enter the **show scp mcast group 127** command or the command might wrongly display some processors to be part of group 127 that are not. This problem is resolved in Release 12.1(13)E5. (CSCdz85864)
- With multicast support configured, a reload might occur when an interface flaps. This problem is resolved in Release 12.1(13)E5. (CSCdy89663)
- If an output route-map in an EBGP neighbor has **match ip next-hop** or **match ip route-source** or **match ip community** or **match ip extcommunity** commands, then BGP updates might be incorrectly suppressed if the next-hop of the best path changes. This problem is resolved in Release 12.1(13)E5. (CSCdv36378)
- With a network topology that creates an assert, after the assert winner prunes its outgoing interface (which is correct), some neighbor routers might fail to override the prune with a join, which might break dense mode auto RP groups.This problem is resolved in Release 12.1(13)E5. (CSCdv23921)

- With a Supervisor Engine 2, if the **show id supervisor** *slot_num* command displays "8006" as part of the "Manufacturing Assembly Number," then all CoS values for the Gigabit Ethernet ports on the Supervisor Engine 2 are mapped to queue 1, threshold 1, by default and cannot be reconfigured. You cannot enter the following commands for the Gigabit Ethernet ports on the Supervisor Engine 2:
  - **wrr-queue cos-map**
  - **rcv-queue cos-map**
  - **priority-queue cos-map**

  This caveat applies only to the Gigabit Ethernet ports on the Supervisor Engine 2. It does not affect any other ports on any other modules. This problem is resolved in Release 12.1(13)E5. (CSCea05105)
- On a Layer 3 EtherChannel, if you apply an ACL to both the port-channel interface and to a member port, the ACL does not deny traffic correctly. This problem is resolved in Release 12.1(13)E5. (CSCdz56987)
- VACL capture does not work if you enter the **mls aclmerge algorithm odm** command. This problem is resolved in Release 12.1(13)E5. (CSCea17364)
- Not all the traps in CISCO-ENTITY-FRU-CONTROL-MIB are supported. This problem is resolved in Release 12.1(13)E5. (CSCea07970)
- A spurious memory access might occur when you copy a file to the disk0 device. This problem is resolved in Release 12.1(13)E5. (CSCdy73395)
- Under heavy traffic load for an extended period, the FIB might be disabled. This problem is resolved in Release 12.1(13)E5. (CSCdy47802)
- With two power supplies in a nonredundant configuration, when one power supply fails and there is insufficient power to support the installed modules, the switch removes power from modules starting with the highest numbered slot, including slots that have service modules installed. Examples of service modules are WS-SVC-CMM, WS-SVC-FWM-1-K9, WS-X6381-IDS, WS-SVC-NAM-2, WS-SVC-NAM-1, WS-X6380-NAM, WS-X6066-SLB-APC, WS-SVC-CSG-1, and WS-SVC-SSL-1. Power is not removed from slots with supervisor engines or SFMs. CSCdy49957 adds service modules to the list of modules exempt from power removal. (CSCdy49957)
- You are able to enter the **broadcast suppression** command in releases where it is not supported and where it does not work. This problem is resolved in Release 12.1(13)E5. (CSCdy84113)
- When nonpolling problems occur, an incorrect "Module not responding to Keep Alive polling" message is displayed. This problem is resolved in Release 12.1(13)E5. (CSCdz21419)
- A reload might occur if you enter the **show tech-support** command through the Catalyst Web Interface (CWI). This problem is resolved in Release 12.1(13)E5. (CSCdz28008)
- Static multicast MAC entries do not work after a reload. This problem is resolved in Release 12.1(13)E5. (CSCdz66347)
- If BGP is advertising a large number of routes and is peering with two different BGP autonomous systems, and with a large input ACL on ports where traffic is received, occasionally BGP might fail to converge when a link to one of the BGP peers is shut down. This problem is resolved in Release 12.1(13)E5. (CSCdz89258)
- When a Supervisor Engine 1 is experiencing high CPU utilization, you might encounter CRC errors when you copy a file to slot0. This problem is resolved in Release 12.1(13)E5. (CSCdz23863)
- In a stub-network topology where the routers are configured in sparse-dense mode, the DR CPU utilization is very high when the CPU receives non-RPF traffic for groups operating in dense mode. When the **mls ip multicast stub** command is configured, the non-DR CPU utilization stays stable. This problem is resolved in Release 12.1(13)E5. (CSCea00720)

- The output packet counter on a VLAN interface displays incorrect information. This problem is resolved in Release 12.1(13)E5. (CSCea02680)
- In a topology with routed interfaces, multicast packets may be lost because of incorrect management of LTL indexes. If you enter a **shutdown** command followed by a **no shutdown** command on the interfaces or perform an OIR of the modules, this problem might occur. This problem is resolved in Release 12.1(13)E5. (CSCea04508)
- The CAM table might lose a static MAC address entry when multicast MAC addresses and unicast IP addresses are used in redundant firewalls. This problem is resolved in Release 12.1(13)E5. (CSCea18561)
- An ACL configured with a "deny udp any any eq 0" ACE blocks noninitial fragmented UDP traffic, although the noninitial fragment packet does not contain a UDP header. This problem is resolved in Release 12.1(13)E5. (CSCea27336)
- If the previously active supervisor engine is not automatically rebooted after an RPR+ switchover, devices may be missing from the ciscoFlashMIB SNMP MIB. This problem is resolved in Release 12.1(13)E5. (CSCea45559)
- With the RADIUS load balancing feature of Cisco IOS server load balancing (Cisco IOS SLB), memory corruption and a system reload might occur if you use the **replicate casa** command or RADIUS sticky objects for high availability. This problem is resolved in Release 12.1(13)E5. (CSCea48170)
- With HSRP and EIGRP configured, the system might not be stable with heavy IP Protocol Independent Multicast (PIM) dense mode traffic. (CSCdz47426)
- To avoid a reload when PIM auto-rendezvous point (AutoRP) or bootstrap router (BSR) is configured, do not enter the **show ip pim rp mapping** command. This problem is resolved in Release 12.1(13)E5. (CSCdy60995)
- To avoid a reload, do not enter the **clear ip igmp group** command while another user is displaying the output from the **show ip igmp group detail** command. This problem is resolved in Release 12.1(13)E5. (CSCdy72767)
- When the route for a prefix is advertised by both BGP and IGP and the BGP session goes down, the IGP route for the prefix takes over and LDP allocates and advertises the label for it. When the BGP session comes up, the LDP session withdraws the label after a 5-minute wait. Traffic is dropped until the label is withdrawn. This problem is resolved in Release 12.1(13)E5. (CSCdx74321)
- With PIM configured and an (S,G) entry with the F flag reset, a directly connected source might not start registering when the source becomes active, and the (S,G) state might time out. This problem is resolved in Release 12.1(13)E5. (CSCdz16276)
- A Multicast Source Discovery Protocol (MSDP) encapsulated packet that receives a type length value (TLV) with more than one source-active (SA) entry count generates data read errors. (CSCdz39544)
- Unicast RPF does not work. This problem is resolved in Release 12.1(13)E5. (CSCdz83820)

Resolved General Caveats in Release 12.1(13)E4

- Numerous "EARL-SP-5-EXCESSIVE_INTR" might be displayed. This problem is resolved in Release 12.1(13)E4. (CSCdz68529)
- Traffic floods incorrectly in a redundant configuration with an EtherChannel configured across both supervisor engines and across different DFC-equipped modules. This problem is resolved in Release 12.1(13)E4. (CSCdz54333)

- Some NAT translations do not expire. This problem is resolved in Release 12.1(13)E4. (CSCdz44155)
- When you remove a GBIC from one port on a module, you receive SNMP traps for all ports on the module. This problem is resolved in Release 12.1(13)E4. (CSCdz37642)
- Cisco IOS server load balancing (Cisco IOS SLB) connectivity might fail following a "%ICC-SP-5-WATERMARK" message. This problem is resolved in Release 12.1(13)E4. (CSCdy37563)
- The SNMP cefcFRUInserted and cefcFRURemoved notifications are not generated when a GBIC is inserted or removed. This problem is resolved in Release 12.1(13)E4. (CSCdy03042)
- Changes in the Unicast routing table can cause an inconsistency between software and hardware programming of the RPF interfaces of specific multicast groups. This inconsistency causes group-specific multicast traffic to be lost. This problem is resolved in Release 12.1(13)E4. (CSCdz44110)
- Some traffic sent through a Layer 2 EtherChannel that includes interfaces on different DFC-equipped switching modules is lost. This problem is resolved in Release 12.1(13)E4. (CSCdz29883)
- Configuring extended range VLANs causes a memory leak. This problem is resolved in Release 12.1(13)E4. (CSCdy46743)
- A Supervisor Engine 1 with an MSFC might display the following message and reload:

  ```
  %RPC-2-FAILED: Failed to send RPC request mapping_sp:get_current_mappings
  ```

  This problem is resolved in Release 12.1(13)E4. (CSCdz50453)
- With multicast routing disabled, multicast traffic is routed through interfaces where PIM is configured. This problem is resolved in Release 12.1(13)E4. (CSCdz42307)
- With ACLs configured, traffic is not routed following a switchover to the redundant supervisor engine. This problem is resolved in Release 12.1(13)E4. (CSCdz55647)
- With BGP routing configured to use parallel links, CPU usage might be 100% for an extended period if the link with the lowest IP address fails. This problem is resolved in Release 12.1(13)E4. (CSCdz79139)
- IGMP snooping fast leave is not honored during the time interval between receipt of a general query and the value of the query response interval (see RFC2236, Section 8.3) contained in the received general query. You can configure the query response interval with the "ip igmp query-max-response-time" interface command. For example, if the query response interval is 10 seconds in the received general query, then the interface command "ip igmp snooping fast-leave" configured on a VLAN interface corresponding to the VLAN on which the query was received has no effect for 10 seconds after this general query is received in this VLAN. In environments with very high IGMP leave rates, IGMP snooping might not process some leave messages. This problem is resolved in Release 12.1(13)E4. (CSCdz65685)

Resolved General Caveats in Release 12.1(13)E3

- Some physical ports in EtherChannels might fail to carry traffic, resulting in unexpected traffic loss. This problem is resolved in Release 12.1(13)E3. (CSCdy48112)
- In a network that is configured for multicast redundancy, which has a high volume of multicast traffic where the last-hop Catalyst 6500 series switches or Cisco 7600 Series Routers are the Anycast RP pair, and SPT threshold infinity is configured, the non-DR router might experience high CPU. This problem is resolved in Release 12.1(13)E3. (CSCdz48825)

- SNMP access of cltcDot1qTunnelMode might cause a reload. This problem is resolved in Release 12.1(13)E3. (CSCdz35749)
- The implementation of the CISCO-SLB-EXT-MIB on the Catalyst 6500 series switches and Cisco 7600 Series Routers does not support the "SET" operation. When a user attempts a "SET" operation on the following objects, the system tries to free unallocated memory and generates traceback messages:
  - cslbxServerFarmHashMaskAddr
  - cslbxServerFarmClientNatPool
  - cslbxServerFarmHttpReturnCodeMap
  - cslbxVirtualURLHashBeginString
  - cslbxVirtualURLHashEndString

  This problem is resolved in Release 12.1(13)E3. (CSCdz54807)
- If the length field in the MSDP TLV is less than the minimum MSDP TLV size (3 bytes), memory corruption might occur and cause the system to reload. This problem is resolved in Release 12.1(13)E3. (CSCdz25339)
- A system with an MSFC2 running a c6msfc2-jsv-mz.121-11b.E4 software image may run out of memory and reload. The **show version** command output may indicate that the system returned to ROM monitor mode. The stack or crash-information log might not be saved. Occasionally after the reload, free memory in the processor pool may start to decrease. IP input is the process that might be using the additional memory. This problem is resolved in Release 12.1(13)E3. (CSCdz18419)
- Cisco IOS SLB does not support RPR+. If you configure Cisco IOS SLB with redundant supervisor engines, you need to configure RPR. This problem is resolved in Release 12.1(13)E3. (CSCdz25527)
- The switch processor may reset because of memory corruption when a race condition occurs between two multicast processes This problem occurs when a multicast router port's hold timer expires and the port link status goes down almost immediately. Both processes try to delete the multicast router port from its database at the same time. This problem is resolved in Release 12.1(13)E3. (CSCdz47758)
- In rare situations, a system running IOS 12.1(8a)E5 may reload with a bus error after you enter the **ip verify unicast reverse-path** command on an interface. This problem is resolved in Release 12.1(13)E3. (CSCdw20764)
- The system may reload because of memory corruption. This problem occurs when SNMP is set to the snmp-set smonVlanIdStatsTable elem 64-bit counter. This problem is resolved in Release 12.1(13)E3. (CSCdw50718)
- If an RPR+ switchover is performed while traffic is forwarded, you may see L3-PS-DRVR switch processor messages on the console. This problem is resolved in Release 12.1(13)E3. (CSCdw71753)
- The hardware FIB may point to an incorrect adjacency entry when a recursive lookup is involved. You can resolve this problem by entering a **clear ip route *** command, which builds the hardware forwarding and adjacency tables again. This problem is resolved in Release 12.1(13)E3. (CSCdx93111)
- The ifOutDiscard counter is updated incorrectly on WS-X6548 LC modules. This problem is resolved in Release 12.1(13)E3. (CSCdz02952)
- Because of a race condition, a (*,G) flow may not be completely switched in hardware. Traffic and forwarding capabilities remain unaffected. This problem is resolved in Release 12.1(13)E3. (CSCdz04555)

- In a configuration that contains many route maps, if you ping from a router to a VLAN interface messages like the following may be displayed and the TCAM screening status may be displayed as INACTIVE:

```
00:03:41: :FM-ODM: Maximum Number of entries exceeded, ODM gives up!
odm_intra_feature_merge:odm_merge fail with code=1

00:03:41: %FM-2-TCAM_MEMORY: Interface Vlan711 processor memory low programming
ingress ACLs
```

  This problem is resolved in Release 12.1(13)E3. (CSCdz16693)

- A unique engine ID needs to be added to NDE version 5 export for traffic from the PFC2 to distinguish it from traffic from the MSFC2. This problem is resolved in Release 12.1(13)E3. (CSCdz27636)
- A system with a WS-X6K-SUP2-2GE and WS-F6K-MSFC2 that is running Release 12.1(13)E may reset when connecting a server to a WS-X6548-RJ-45. This problem is resolved in Release 12.1(13)E3. (CSCdz29085)
- If you use a script to remotely login to a Catalyst 6500 series switch or a Cisco 7600 series router, the system may experience a memory leak. This problem is resolved in Release 12.1(13)E3. (CSCdz30206)
- A system with a Supervisor Engine 1 and an MSFC2 does not allow the flow mask to be set to full flow. This problem is resolved in Release 12.1(13)E3. (CSCdz30894)
- When you configure the IOS server load balancing feature called RADIUS load balancing on multiple virtual servers with the **sticky radius framed-ip** command, some RADIUS framed-ip sticky database entries may be deleted prematurely, and stateful backup may not operate correctly. The problem occurs for framed-ip sticky database entries that are created as a result of processing RADIUS packets associated with any virtual server that is not the first virtual server brought into service with framed-ip sticky configured. This problem is resolved in Release 12.1(13)E3. (CSCdz34575)
- Entering a **client** virtual server Cisco IOS SLB configuration command hangs the system. This problem is resolved in Release 12.1(13)E3. (CSCdz37802)
- A Cisco 7603 running Release 1.1(11b)E1 reloads when you configure Cisco IOS SLB. This problem is resolved in Release 12.1(13)E3. (CSCdz51826)
- When adding 1000 VLANs, VTP calculates the download buffer size and if the size is over 64k, a memory corruption might occur causing the system to reset. This problem is resolved in Release 12.1(13)E3. (CSCdz54132)
- When a ping for a multicast group reaches a Supervisor Engine 1 system that has the **ip igmp join-group** command configured on the interface, a (S,G) entry is created and a shortcut is downloaded. For subsequent pings, duplicate replies are sent because the Supervisor Engine 1 forwards two packets to the MSFC, which then sends out two Unicast replies to the source. This problem is resolved in Release 12.1(13)E3. (CSCin24629)
- If you access the ifEntry MIB through SNMP and at the same time delete VLANs through the CLI, the system may reset. This problem has been fixed in and after Release 12.1(13)E3. (CSCdx89085)
- The following message may display:

```
%LINK-SP-2-NOSOURCE: Source idb not set-Process= "<interrupt level>", ipl= 1,
pid= 78 -Traceback=XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
```

  This problem is resolved in Release 12.1(13)E3. (CSCdy18548)

- When a multicast host sends a leave message, the multicast stream is not immediately terminated if a general query has just taken place. This problem is resolved in Release 12.1(13)E3. (CSCdy56062)

Resolved General Caveats in Release 12.1(13)E1

- The L3Capture2 diagnostic test might fail during bootup. This problem is resolved in Release 12.1(13)E1. (CSCdy30707)
- If you enter the **clear ip mroute** command, data corruption occurs in the PIM process and a reload might occur. This problem is resolved in Release 12.1(13)E1. (CSCdx72670)
- A CPU hog condition might cause a reload when the **snmp-server community** global configuration command is executed with several thousands of logical entities configured. This problem is resolved in Release 12.1(13)E1. (CSCdx68230)
- A Cisco Router that has run out of processor memory may unexpectedly reload due to a bus error at an invalid address if there is an attempt to connect with secure shell (ssh) into a vty port, which fails due to a process creation failure. A SYS-2-CFORKMEM error message appears before the restart. This problem is resolved in Release 12.1(13)E1. (CSCdt13023)
- Following a number of "-SP-" malloc-related error messages, the supervisor engine might run out of memory and reload. This problem is resolved in Release 12.1(13)E1. (CSCdz18216)
- A reload occurs when you disable IGMP snooping. This problem is resolved in Release 12.1(13)E1. (CSCdy89124)
- With Supervisor Engine 2, multicast packets that set the router alert option, like IGMP general queries and membership reports, might not be handled properly, which might disrupt IGMP client connectivity. This problem is resolved in Release 12.1(13)E1. (CSCdy84078)
- When the **failaction radius reassign** command has not been entered and the real server fails, Cisco IOS SLB RADIUS Load Balancing incorrectly chooses a different real server to load balance RADIUS interim accounting requests. This problem is resolved in Release 12.1(13)E1. (CSCdy67824)
- If you configure an EtherChannel between the Catalyst operating system and IOS on the supervisor engine and MSFC, the last port on the IOS device might not completely join the EtherChannel, which prevents multicast traffic from using the last port. This problem is resolved in Release 12.1(13)E1. (CSCdy63364)
- Slow replication of conn, sticky, and radius tables occurs when the tables are large and the primary Cisco IOS SLB is preempting the secondary in a stateful configuration. This problem is resolved in Release 12.1(13)E1. (CSCdy60253)
- With Supervisor Engine 2, packet loss might occur for a few seconds after routing protocol multicast packets are received. This problem is resolved in Release 12.1(13)E1. (CSCdy58383)
- When IGMP snooping is enabled on a switch that is between a multicast source and a multicast receiver, the switch incorrectly sends out two mtrace requests for each non-DVMRP-encapsulated mtrace request it receives. This problem is resolved in Release 12.1(13)E1. (CSCdy47269)
- With a Supervisor Engine 2 and a multicast receiver attached through a Layer 3 port on a WS-X6816-GBIC module and another receiver for the same multicast groups attached through a Layer 2 switchport, after a reset of the x6816 module, the Layer 3 port does not forward multicast traffic; or occasionally any forwarded multicast traffic is switched in software. This problem is resolved in Release 12.1(13)E1. (CSCdy60173)
- In rare situations, an MSFC2 might freeze when it can receive control traffic from the supervisor engine, but it cannot send it. This problem is resolved in Release 12.1(13)E1. (CSCdy15598)
- A reload might occur when you enter the **no ip routing** command. This problem is resolved in Release 12.1(8b)E14. (CSCdy02831)
- A reload might occur following a "%ALIGN-1-FATAL" message. This problem is resolved in Release 12.1(13)E1. (CSCdx22902)

- With a Supervisor Engine 2, (*,G) multicast entries are not programmed in hardware. This problem is resolved in Release 12.1(13)E1. (CSCdy44937)
- The messages about the maximum number of logical interfaces are incorrect (see the "Spanning Tree Troubleshooting" section on page 321). This problem is resolved in Release 12.1(13)E1. (CSCdy83667)
- If a DFC fails immediately after it comes online, the system might reload and generate this error message:

  ```
  HEARTBEAT NOT_RUNNING.
  ```

  This problem is most likely to occur during a system boot up or switchover. This problem is resolved in Release 12.1(13)E1. (CSCdy72533)
- Access lists might disappear from the running-config file following a reload. This problem is resolved in Release 12.1(13)E1. (CSCdx52334)
- The following error messages are displayed immediately after a reload:

  ```
  %SYS-2-INTSCHED: 'sleep for' at level 3 -Process= "Init", ipl= 3, pid= 2 -Traceback=
  6064AA94 60633C04 60FFD1C4 611867AC 6066D1CC 60596134 603D1EB0 603D30BC
  603C3110 603D1C20 603BCB30601F2480 601F0460 601F09F0 601F0840 60599A60
  ```

  The **ip cef** global configuration command and the police settings are class-map configurations and need to have a packet identification mechanism before anything is policed (such as match protocol http). This condition does not occur until the policy map is attached to an interface. This symptom is observed after a reload after it had been configured with the following commands:

  ```
  ip cef
       policy-map test-policy
         class-map test-class
           match protocol http
           police cir 64000 bc 16000 pir 64000 be 16000
           conform-action set-clp-transmit
           exceed-action set-clp-transmit
           violate-action set-clp-transmit
       interface e3/1
         service-policy input test-policy
  ```

  This problem is resolved in Release 12.1(13)E1. (CSCdw20801)
- MAC addresses with the routed MAC bit set (Routed MAC part of Layer 3 shortcut) do not age out based on the VLAN aging timer. If the routed MAC aging time is modified from the default value, the VLAN aging time is not used. This problem is resolved in Release 12.1(13)E1. (CSCdy33647)
- In specific oversubscription scenarios, prioritization mechanisms across the fabric do not function properly. This problem is resolved in Release 12.1(13)E1. (CSCdy48208)
- In Release 12.1(13)E, ports with GBICs that have a bad GBIC EEPROM checksum are not allowed to come up. The following error message is printed when this error occurs in the 12.1(13)E release:

  ```
  %PM_SCP-SP-3-GBIC_BAD: GBIC integrity check on port 1/2 failed: bad key
  ```

  The **show interface status** command displays the following output:

  ```
  Router# show int status
  Port    Name               Status       Vlan       Duplex  Speed Type
  Gi2/1                      faulty       routed       full   1000 bad EEPROM
  ```

  This problem is resolved in Release 12.1(13)E1. (CSCdy68962)

- Systems running a Release prior to 12.1(13)E1 might display the following message and reload:

```
%ALIGN-1-FATAL: Illegal access to a low address" 02:58:35:
%IPC-SP-5-INVALID: Seat in Update Last Ack Sequence=0x6F4F-Traceback=
401DE764 401DF8D8 4018BF0C 40189B28 40189D60 40116DD4 05:40:15:
%IPC-SP-5-INVALID: Seat in Update Last Ack Sequence=0xCAC9-Traceback=
401DE764 401DF8D8 4018BF0C 40189B28 40189D60 40116DD4
%ALIGN-1-FATAL: Illegal access to a low address addr=0x39,
pc=0x401DE740, ra=0x401DE71C, sp=0x42DC10A8
```

  This problem is resolved in Release 12.1(13)E1. (CSCdy87300)

- When hardware switching is enabled, packets for (S,G) PR bit entry are not installed in hardware and are not forwarded using the (*,G) entry. This problem is resolved in Release 12.1(13)E1. (CSCdy73313)
- An incorrect traceback message is generated during boot up or reload of a system running Release 12.1(13)E. This problem is resolved in Release 12.1(13)E1. (CSCdy79272)
- When you enter the **ip igmp snooping** and **no ip igmp snooping** interface commands on a VLAN interface in a system running Release 12.1(13)E, the configuration is applied globally and the interface configuration mode changes to global configuration mode. This problem is resolved in Release 12.1(13)E1. (CSCdy87384)
- The ACL command keyword **established** does not work with PFC2. This problem is resolved in Release 12.1(13)E1. (CSCdz00544)
- Port channel configuration may be lost after an RPR+ forced switchover. This problem is resolved in Release 12.1(13)E1. (CSCdz10789)

Resolved General Caveats in Release 12.1(13)E

- The drop counters on Gigabit Ethernet interfaces might incorrectly increment excessively, even during low traffic conditions. No data is actually dropped. This problem is resolved in Release 12.1(13)E. (CSCdv86024)
- There is no Layer 3 hardware-switching support for multicast traffic that needs to be fragmented and which passes through ingress and egress interfaces that have different MTU sizes. This problem is resolved in Release 12.1(13)E. (CSCdx95080)
- If a (S,G) state is created by receiving a prune at the source's first hop router, and then if the source starts sending, the registering process does not occur, which leads to the loss of multicast traffic. This usually happens when the source was sending traffic initially, and then stopped sending, and then starts sending again. This problem is resolved in Release 12.1(13)E. (CSCdw71336)
- A reload might occur when you enter the **show ip mroute** command. This problem is resolved in Release 12.1(13)E. (CSCdx79227)
- Following a **reload** command, the redundant supervisor engine might not boot properly. This problem is resolved in Release 12.1(13)E. (CSCdw39543)
- With a Supervisor Engine 1, some traffic that does not match the routing policy is policy routed. This problem is resolved in Release 12.1(13)E. (CSCdx17428)
- A reload might occur while displaying the group-rp mapping cache. This problem is resolved in Release 12.1(13)E. (CSCdw16433)
- The IGMP ROBUSTNESS_VAR is increased from 1 to 2 in Release 12.1(13)E. (CSCdt45806)
- With Cisco IOS SLB configured, a reload might occur following these messages: "Unexpected exception, CPU signal 10, PC = 0x602D8934" or "%ALIGN-1-FATAL." This problem is resolved in Release 12.1(13)E. (CSCdy40171)

- With IGMP snooping enabled, the system does not learn router ports from IGMP membership queries. This problem is resolved in Release 12.1(13)E. (CSCdx39149)
- When the MSFC is the IGMP querier on a Layer 3 interface and it receives a topology change notification (TCN), the MSFC does not send the required general queries when only IGMP is enabled. The MSFC sends the two general queries, spaced 10 seconds apart, only if CGMP is enabled. This problem is resolved in Release 12.1(13)E. (CSCdx42565)
- Slowly inserting or removing a module might freeze the system in a switching bus stall. This problem is resolved in Release 12.1(13)E. (CSCdy19226)
- If you enter the **no mls qos** command to disable QoS on a Layer 2 port that is configured for VLAN-based QoS with the **mls qos vlan-based** command, any policies applied to the port's VLAN continue to be applied to traffic coming from the port. This problem is resolved in Release 12.1(13)E. (CSCdy26824)
- With a PFC2 and with DFCs, you cannot configure Layer 2 EtherChannels that include interfaces on different DFC-equipped switching modules. This problem is resolved in Release 12.1(13)E. (CSCdt27074)
- If you enter the **do** command under the **interface range** command, Cisco IOS executes the **do** command for each interface in the range. This problem is resolved in Release 12.1(13)E. (CSCdw92111)
- In a system that has policing configured and a Switch Fabric Module installed, the "AgId" field is reset to zero in the display after an OIR of a Switch Fabric Module, and the counters may not show packets that are policed. This problem is resolved in Release 12.1(13)E. (CSCdy19696)
- You cannot configure a port on a fabric-enabled switching module as a SPAN source port. This problem is resolved in Release 12.1(13)E. (CSCdw74764)
- Because of a lack of IPC buffer space, a system with a Supervisor Engine 1 and an MSFC2 might reload when ICC messages are waiting in the queue. Before the system reloads, messages of the following type may appear:

  ```
  %ICC-SP-5-WATERMARK:5988 pkts for class L3-MGR are waiting to be processed
  %IPC-SP-3-NOBUFF:The main IPC message header cache has emptied
  ```

  This problem is resolved in Release 12.1(13)E. (CSCdw53279, CSCdx05096)
- IP connectivity to the supervisor engine Gigabit Ethernet ports does not work in Releases 12.1(11b)E and 12.1(11b)E1. This problem is resolved in Release 12.1(13)E. (CSCdx04363)
- With loose Unicast RPF configured on the MSFC, traffic that should be dropped is still forwarded through the MSFC. This problem is resolved in Release 12.1(13)E. (CSCdw92775)
- In a PFC2/MSFC2 system with a fabric-enabled, 48-port, 10/100 Mbps, RJ45 module and a fabric-enabled, 16-port, 1000 Mbps, GBIC module installed, when traffic enters the fabric-enabled, 48-port, 10/100 Mbps, RJ45 and exits through the fabric-enabled, 16-port, 1000 Mbps GBIC module, or in the other direction, dCEF forwarding is not enabled on the ingress module and traffic is dropped at the ingress port. This problem is resolved in Release 12.1(13)E. (CSCdw55635)
- If you enter the **do** command under the **interface range** command, Cisco IOS executes the **do** command for each interface in the range. This problem is resolved in Release 12.1(13)E. (CSCdw92111)
- To avoid unreliable operation, do not enter the **do** command in EXEC mode. This problem is resolved in Release 12.1(13)E. (CSCdx02925)

- Packets between fabric-enabled modules can be forwarded from one module to another using either the 8-Gigabit Ethernet fabric interface or the 16-Gigabit Ethernet backplane bus. In a system where fewer than 3 fabric-enabled modules are installed, replicated multicast packets are occasionally sent over the fabric as well as over the backplane bus, which causes ports to receive twice as many packets as were generated. This problem is resolved in Release 12.1(13)E. (CSCdw82490)
- The WS-CAC-2500W power supply supplies 1153.32 W at 110 V, but the **show power** command incorrectly shows an output of 2331.00 W. This problem is resolved in Release 12.1(13)E. (CSCdx69850)
- For Layer 2 VLANs, Layer 3 VLAN interfaces, and Layer 3 router ports, Supervisor Engine 2 exports per-interface switching statistics to the MSFC2 approximately every 3 minutes, which delays the availability of the statistics but does not affect their completeness or accuracy. This problem is resolved in Release 12.1(13)E. (CSCdw88399)
- If you configure a port with a VACL access map that has an action clause that contains the **capture** keyword, the port does not send any traffic to the MSFC for processing in software, which prevents support of features such as the following:
  - Cisco IOS ACL log
  - NAT
  - PBR
  - Cisco IOS server load balancing (Cisco IOS SLB)
  - WCCP
  - CBAC
  - TCP intercept

  This problem is resolved in Release 12.1(13)E. (CSCdu61309, CSCdx37625)
- PFC QoS supports class maps that contain a single **match** command. PFC QoS incorrectly fails to reject a policy map that contains a class configured with multiple **match** commands if the subsequent **match** commands refer to undefined ACLs and the class is configured with a microflow policer but not with an aggregate policer. PFC QoS uses the first **match** command and ignores the others. This problem is resolved in Release 12.1(13)E. (CSCdw26679)
- If the shared tree and the shortest path tree (SPT) diverge because of a Reverse Path Forwarding (RPF) change on the shared tree (normally triggered by a restoration of a failed link), the SPT is pruned. A join to restore the traffic flow immediately follows the prune, which might interrupt traffic briefly. This problem is resolved in Release 12.1(13)E. (CSCdu74664)
- MAC address notifications to Layer 3 EtherChannels can be sent to the wrong ingress switching module. This problem is resolved in Release 12.1(13)E. (CSCdy47285)
- Nonmaskable interrupts (NMIs) might cause a Supervisor Engine 1 to reload, and then the reload might fail. This problem is resolved in Release 12.1(13)E. (CSCdy25902)
- A failure in communication between the MSFC and supervisor engine causes the MSFC to be reset by an internal message from the supervisor engine. This problem is resolved in Release 12.1(13)E. (CSCdx38960)
- If you configure an active member port of an EtherChannel as a SPAN source port, the port goes into the suspended state and does not pass any traffic. In Release 12.1(13)E, you cannot configure an active member port of an EtherChannel as a SPAN source port. (CSCdx81246)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(13)E17, page 252
- Resolved FlexWAN Module Caveats in Release 12.1(13)E17, page 252
- Resolved FlexWAN Module Caveats in Release 12.1(13)E16, page 252
- Resolved FlexWAN Module Caveats in Release 12.1(13)E15, page 252
- Resolved FlexWAN Module Caveats in Release 12.1(13)E14, page 253
- Resolved FlexWAN Module Caveats in Release 12.1(13)E13, page 253
- Resolved FlexWAN Module Caveats in Release 12.1(13)E12, page 253
- Resolved FlexWAN Module Caveats in Release 12.1(13)E11, page 253
- Resolved FlexWAN Module Caveats in Release 12.1(13)E10, page 253
- Resolved FlexWAN Module Caveats in Release 12.1(13)E9, page 253
- Resolved FlexWAN Module Caveats in Release 12.1(13)E8, page 253
- Resolved FlexWAN Module Caveats in Release 12.1(13)E7, page 254
- Resolved FlexWAN Module Caveats in Release 12.1(13)E6, page 254
- Resolved FlexWAN Module Caveats in Release 12.1(13)E5, page 254
- Resolved FlexWAN Module Caveats in Release 12.1(13)E4, page 254
- Resolved FlexWAN Module Caveats in Release 12.1(13)E3, page 254
- Resolved FlexWAN Module Caveats in Release 12.1(13)E1, page 254
- Resolved FlexWAN Module Caveats in Release 12.1(13)E, page 255

Open FlexWAN Module Caveats in Release 12.1(13)E17

- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan** *slot_number/port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module crashinfo file with the **copy cwan** *slot_number/port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)

Resolved FlexWAN Module Caveats in Release 12.1(13)E17

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E16

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E15

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E14

- With a high traffic load, PA-A3-OC3, PA-A3-T3, and PA-A3-E3 port adapters might display an increasing "rx_no_buffer" counter in the output of the **show controllers atm** privileged EXEC command and some PVCs configured on the PA-A3 port adapter might stop receiving traffic. This problem is resolved in Release 12.1(13)E14. (CSCin49458)
- All high-capacity counters remain at 0 for FlexWAN module POS interfaces. This problem is resolved in Release 12.1(13)E14. (CSCdz46845)
- In a system installed with a FlexWAN and a PA-A3 ATM port adapter, the ATM interface may stay down after you enter a **shutdown** command followed immediately by a **no shutdown** command. This problem is resolved in Release 12.1(13)E14. (CSCdw65799)

Resolved FlexWAN Module Caveats in Release 12.1(13)E13

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E12

- ATM subinterface traffic might be incorrectly dropped. This problem is resolved in Release 12.1(13)E12. (CSCea81118

Resolved FlexWAN Module Caveats in Release 12.1(13)E11

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E10

- When you configure IP precedence to ATM CoS mapping in a bundle on a FlexWAN ATM port adapter, the precedence mapping does not work if you specify a range of precedences under a VC in the bundle. The bundle only forwards the first precedence in the range. This problem is resolved in Release 12.1(13)E10. (CSCea56687)
- A reload might occur if there are multiple sessions configuring an ATM interface at the same time. This problem is resolved in Release 12.1(13)E10. (CSCdr61944)
- When you configure an ATM subinterface, it does not inherit the MTU size of the physical interface. When you change the MTU on the physical interface, ATM subinterfaces do not inherit the changed MTU size. This problem is resolved in Release 12.1(13)E10. (CSCea86866)
- VPN does not work on multilink PPP (MLPPP) interfaces. This problem is resolved in Release 12.1(13)E10. (CSCea37725)

Resolved FlexWAN Module Caveats in Release 12.1(13)E9

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E8

- A FlexWAN module might reload after entering **shutdown** and **no shutdown** commands on PA-A3-OC3, PA-A3-T3, or PA-A3-E3 interfaces. This problem is resolved in Release 12.1(13)E8. (CSCea17496)

Resolved FlexWAN Module Caveats in Release 12.1(13)E7

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E6

None.

Resolved FlexWAN Module Caveats in Release 12.1(13)E5

- For channelized T1 interfaces, the following counters do not increment correctly:
  - The “bytes in” and “bytes out” counts displayed by the **show frame pvc** command.
  - The point-to-point pvc subinterface statistics gathered through SNMP for ifInOctets and ifOutOctets
  - The pvc statistics gathered through SNMP for frCircuitReceivedOctets and frCircuitSentOctets
  - The pvc statistics gathered through SNMP for cfrExtCircuitUncompressIns and cfrExtCircuitUncompressOuts

  This problem is resolved in Release 12.1(13)E5. (CSCdz38136)
- For HSSI interfaces, the 5-minute output rate displayed by the **show interface** command does not increment correctly. This problem is resolved in Release 12.1(13)E5. (CSCdz76961)

Resolved FlexWAN Module Caveats in Release 12.1(13)E4

- ATM VC bundling precedence mapping does not work. This problem is resolved in Release 12.1(13)E4. (CSCdz61586)
- MPLS traffic drops when one E1 link of a multilink bundle fails on a PA-MC-8E1/120 port adapter. This problem is resolved in Release 12.1(13)E4. (CSCdy76871)

Resolved FlexWAN Module Caveats in Release 12.1(13)E3

- After an OIR, a FlexWAN module may fail to save a crash-information file after a reset if it has a Packet-over-SONET (POS) port adapter with 500 Frame Relay point-to-point DLCIs in Bay 0 and an ATM port adapter with 500 point-to-point operation, administration, and maintenance PVCs in Bay 1. This problem is resolved in Release 12.1(13)E3. (CSCdy18458, CSCdy09631)
- FlexWAN interfaces may go down suddenly and randomly, with the following message on the MSFC2 console on a Cisco 7600 series router:

  ```
  CBUS-3_CMDTIMEOUT: cmd timed out, CCB 0x0, slot <slot-num>, cmd code <number>
  ```

  Interfaces will come up if you enter a **shutdown** command followed by a n**o shutdown** command. This problem is resolved in Release 12.1(13)E3. (CSCdy81389)

Resolved FlexWAN Module Caveats in Release 12.1(13)E1

- After you move multilink members from one FlexWAN module to another, traffic does not pass through the multilink interface. This problem is resolved in Release 12.1(13)E1. (CSCdy24019)

- An ALIGN-1-FATAL:RSP_update_linecard_vc_blt_state message might be displayed, followed by a reload. This problem is resolved in Release 12.1(13)E1. (CSCdy17228)
- Because of an inter-process communication failure on the MSFC, the supervisor engine might reset after switched virtual circuit (SVC) traffic is forwarded on a FlexWAN ATM port adapter. This problem is resolved in Release 12.1(13)E1. (CSCdy18390)

Resolved FlexWAN Module Caveats in Release 12.1(13)E

None.

Service Modules Caveats

- Open Service Modules Caveats in Release 12.1(13)E17, page 255
- Resolved Service Module Caveats in Release 12.1(13)E17, page 256
- Resolved Service Module Caveats in Release 12.1(13)E16, page 256
- Resolved Service Module Caveats in Release 12.1(13)E15, page 256
- Resolved Service Module Caveats in Release 12.1(13)E14, page 256
- Resolved Service Module Caveats in Release 12.1(13)E13, page 256
- Resolved Service Module Caveats in Release 12.1(13)E12, page 256
- Resolved Service Module Caveats in Release 12.1(13)E11, page 256
- Resolved Service Module Caveats in Release 12.1(13)E10, page 256
- Resolved Service Module Caveats in Release 12.1(13)E9, page 256
- Resolved Service Module Caveats in Release 12.1(13)E8, page 256
- Resolved Service Module Caveats in Release 12.1(13)E7, page 256
- Resolved Service Module Caveats in Release 12.1(13)E6, page 256
- Resolved Service Module Caveats in Release 12.1(13)E5, page 257
- Resolved Service Module Caveats in Release 12.1(13)E4, page 257
- Resolved Service Module Caveats in Release 12.1(13)E3, page 257
- Resolved Service Module Caveats in Release 12.1(13)E1, page 257
- Resolved Service Module Caveats in Release 12.1(13)E, page 257

Open Service Modules Caveats in Release 12.1(13)E17

- In a chassis with four SSL modules installed, if you reload the entire chassis, one of the SSL modules may to fail to come online and power may not to be allocated to the module.

  Workaround: Power cycle the failed SSL module. (CSCdy58630)

  Note CSCdy58630 is not seen in later releases.

- To avoid an MSFC reload, do not enter the **firewall vlan-group** command with VLAN IDs greater than 4094. This problem is resolved in Release 12.1(14)E. (CSCdy39310)
- Do not define VLANs 1002 through 1005 as secure VLANs with the **firewall vlan-group** command. This problem is resolved in Release 12.1(14)E. (CSCdx88498)

Resolved Service Module Caveats in Release 12.1(13)E17

None.

Resolved Service Module Caveats in Release 12.1(13)E16

None.

Resolved Service Module Caveats in Release 12.1(13)E15

None.

Resolved Service Module Caveats in Release 12.1(13)E14

None.

Resolved Service Module Caveats in Release 12.1(13)E13

None.

Resolved Service Module Caveats in Release 12.1(13)E12

None.

Resolved Service Module Caveats in Release 12.1(13)E11

None.

Resolved Service Module Caveats in Release 12.1(13)E10

None.

Resolved Service Module Caveats in Release 12.1(13)E9

None.

Resolved Service Module Caveats in Release 12.1(13)E8

None.

Resolved Service Module Caveats in Release 12.1(13)E7

- The VLAN autostate behavior is not correct with a WS-SVC-NAM-2 module installed and configured. This problem is resolved in Release 12.1(13)E7. (CSCea71694)
- Except when using the console connection, a reload might occur when you try to configure a WS-X6066-SLB-APC module. This problem is resolved in Release 12.1(13)E7. (CSCeb00678)

Resolved Service Module Caveats in Release 12.1(13)E6

None.

Resolved Service Module Caveats in Release 12.1(13)E5

None.

Resolved Service Module Caveats in Release 12.1(13)E4

None.

Resolved Service Module Caveats in Release 12.1(13)E3

- To avoid a reload, do not enter the **show firewall module** *module_number* **stat** command while the WS-SVC-FWM-1-K9 Firewall Services Module is resetting. This problem was resolved in Release 12.1(13)E3. (CSCdy53164)

Resolved Service Module Caveats in Release 12.1(13)E1

- If you insert an SSL module into a slot that was previously occupied by a DFC, the SSL module will not come online. This problem is resolved in Release 12.1(13)E1. (CSCdy53696)

Resolved Service Module Caveats in Release 12.1(13)E

None.

OSM Caveats

- Open OSM Caveats in Release 12.1(13)E17, page 257
- Resolved OSM Caveats in Release 12.1(13)E17, page 258
- Resolved OSM Caveats in Release 12.1(13)E16, page 258
- Resolved OSM Caveats in Release 12.1(13)E15, page 258
- Resolved OSM Caveats in Release 12.1(13)E14, page 258
- Resolved OSM Caveats in Release 12.1(13)E13, page 258
- Resolved OSM Caveats in Release 12.1(13)E12, page 258
- Resolved OSM Caveats in Release 12.1(13)E11, page 258
- Resolved OSM Caveats in Release 12.1(13)E10, page 258
- Resolved OSM Caveats in Release 12.1(13)E9, page 259
- Resolved OSM Caveats in Release 12.1(13)E8, page 259
- Resolved OSM Caveats in Release 12.1(13)E7, page 259
- Resolved OSM Caveats in Release 12.1(13)E6, page 259
- Resolved OSM Caveats in Release 12.1(13)E5, page 259
- Resolved OSM Caveats in Release 12.1(13)E4, page 260
- Resolved OSM Caveats in Release 12.1(13)E3, page 261
- Resolved OSM Caveats in Release 12.1(13)E1, page 261

Open OSM Caveats in Release 12.1(13)E17

None.

Resolved OSM Caveats in Release 12.1(13)E17

None.

Resolved OSM Caveats in Release 12.1(13)E16

None.

Resolved OSM Caveats in Release 12.1(13)E15

- An OSM might be reset following an online insertion and removal (OIR) of a Switch Fabric Module (SFM) or during periods of heavy traffic. This problem is resolved in Release 12.1(13)E15. (CSCin37112)
- Traffic loss might occur on OSMs when there are frequent OIRs. This problem is resolved in Release 12.1(13)E15. (CSCee54642)
- Multicast 127-byte UDP packets that egress from OSM-2OC12-POS interfaces have invalid checksums. This problem is resolved in Release 12.1(13)E15. (CSCec72798)

Resolved OSM Caveats in Release 12.1(13)E14

- Occasionally, OSM POS interfaces stop updating statistics while traffic is passing. This problem is resolved in Release 12.1(13)E14. (CSCea78519)

Resolved OSM Caveats in Release 12.1(13)E13

- Directed broadcasts to a destination network that is part of an MPLS VPN fail.This problem is resolved in Release 12.1(13)E13. (CSCec75499)

Resolved OSM Caveats in Release 12.1(13)E12

- An ATM OSM module does not route packets between bridged RFC 1483 PVCs that are configured in different VLANs. This problem is resolved in Release 12.1(13)E12. (CSCea84940)
- An E3 link to an OC-12 channelized OSM might not come up. This problem is resolved in Release 12.1(13)E12. (CSCec39689)

Resolved OSM Caveats in Release 12.1(13)E11

None.

Resolved OSM Caveats in Release 12.1(13)E10

- Following a reload, it is safe to ignore this message from OSM-2OC12-POS-MM, OSM-2OC12-POS-SI, or OSM-2OC12-POS-SL modules in a fully loaded chassis:

  ```
  %SM-SP-4-BADEVENT: Event 'dnld_completed' is invalid for the current state
  'online': scp_dnld_module 4
  ```

  This problem is resolved in Release 12.1(13)E10. (CSCdw10533)
- A reload might occur if there are multiple sessions configuring an ATM interface at the same time. This problem is resolved in Release 12.1(13)E10. (CSCdr61944)

- When you configure an ATM subinterface, it does not inherit the MTU size of the physical interface. When you change the MTU on the physical interface, ATM subinterfaces do not inherit the changed MTU size. This problem is resolved in Release 12.1(13)E10. (CSCea86866)
- EoMPLS VCs flap on an 8-port, 8 Gbps customer edge-to-provider edge (CE-to-PE) router connection between WS-X6516-GBIC and OSM-2+4GE-WAN+ modules. This problem is resolved in Release 12.1(13)E10. (CSCeb04954)
- The FIB on an OSM might not be synchronized with the FIB on the MSFC. This problem is resolved in Release 12.1(13)E10. (CSCeb52142)
- When an OSPF topology change occurs, an MPLS provider edge (PE) router might not forward IP-to-Tag traffic to some IP destinations when it has equal cost load-sharing paths to the IP destinations. This problem is resolved in Release 12.1(13)E10. (CSCeb52169)
- The 64-bit SNMP counters on OSM-4GE-WAN and OSM-2+4GE-WAN+ modules behave like 32-bit counters. This problem is resolved in Release 12.1(13)E10. (CSCeb60961)

Resolved OSM Caveats in Release 12.1(13)E9

None.

Resolved OSM Caveats in Release 12.1(13)E8

None.

Resolved OSM Caveats in Release 12.1(13)E7

- Because subinterfaces on the OSM-2+4GE-WAN+ module cannot share HSRP group numbers, the 4-port Gigabit Ethernet WAN module supports only 16 HSRP groups per Gigabit Ethernet WAN port. This problem is resolved in Release 12.1(13)E7. (CSCeb11624)
- An SNMP poll returns “NO_SUCH_INSTANCE_EXCEPTION” for the OSM-4GE-WAN-GBIC and OSM-2+4GE-WAN+ broadcast and multicast packet high-capacity counters. This problem is resolved in Release 12.1(13)E7. (CSCea59922)
- The Gigabit Ethernet ports on the OC-48 OSMs may experience output drops. This problem is resolved in Release 12.1(13)E7. (CSCea76234)
- When an EoMPLS VC is configured on an OSM, the output counter and some interface MIB counters display incorrect values. This problem is resolved in Release 12.1(13)E7. (CSCeb04036)
- The **set mpls exp** and **set ip precedence** commands are not supported with basic MPLS and MPLS VPN. This problem is resolved in Release 12.1(13)E7. (CSCin43408, CSCeb25018)

Resolved OSM Caveats in Release 12.1(13)E6

None.

Resolved OSM Caveats in Release 12.1(13)E5

- You cannot configure both HSRP and an override MAC address on OSM-4GE-WAN module or OSM-2+4GE-WAN+ module interfaces. This problem is resolved in Release 12.1(13)E5. (CSCea59633)
- Ethernet packets with non-standards compliant source addresses might cause a provider edge (PE) router to reload. This problem is resolved in Release 12.1(13)E5. (CSCea41242)

- When an HSRP group is configured on a OSM-4GE-WAN subinterface and MPLS VPN is configured on the same subinterface, packet duplication might occur. This problem is resolved in Release 12.1(13)E5. (CSCea21791)
- The OSM-4GE-WAN-GBIC module returns an incorrect port type value in CiscoView. This problem is resolved in Release 12.1(13)E5. (CSCea28575)
- The interface Link Up/Down SNMP trap is not generated for subinterfaces on the OSM-4GE-WAN-GBIC module after you enter a **shutdown** command followed by a **no shutdown** command on the subinterface or main interface. This problem is resolved in Release 12.1(13)E5. (CSCea42741)
- On ATM and POS OSM modules when the system comes up, the portType is displayed as "other" if no GBIC is present in the Gigabit Ethernet ports. On the Gigabit Ethernet WAN OSMs, when a GBIC is removed, the portType displays "other." This problem is resolved in Release 12.1(13)E5. (CSCin37330)
- Packets to an unknown MAC address that exists in the same subnet as a GE-WAN VPN routing and forwarding (VRF) subinterface are incorrectly accepted by the GE-WAN subinterface and then routed back to the VLAN. If there are two GE-WAN VRF subinterfaces configured for the same VLAN for redundancy, packets are forwarded back and forth between the GE-WAN subinterfaces until the TTL timer expires. This may cause problems for applications in the subnet and on the hosts involved. This problem is resolved in Release 12.1(13)E5. (CSCea45053)
- The OSM-12CT3/T1 and OSM-CHOC12/T1-SI modules do not support wire-rate traffic on serial interfaces. This problem is resolved in Release 12.1(13)E5. (CSCdz46704)
- Input-shaping policies on OSMs shape at a lower rate than the configured rate. This problem is resolved in Release 12.1(13)E5. (CSCdy15369)
- On an OSM-2+4GE-WAN+ module, if you apply a nonhierarchical service policy to the physical port 2 or port 4 interface when port 1 or port 3 is shutdown, the service-policy application fails without notice. This problem is resolved in Release 12.1(13)E5. (CSCdz57493)
- The OSM-2+4GE-WAN+ module does not support WS-G5483 GBICs. This problem is resolved in Release 12.1(13)E5. (CSCdz88585)
- On a GE-WAN port configured as a Layer 3 trunk, if you change the encapsulation from ISL to IEEE 802.1Q or from IEEE 802.1Q to ISL, all trunk traffic is routed in software by the MSFC2. This problem is resolved in Release 12.1(13)E5. (CSCdz89162)

Resolved OSM Caveats in Release 12.1(13)E4

- Automatic Protection Switching (APS) switchover on OSM-1CHOC12/T1-SI modules configured with multilink point-to-point protocol (MLPPP) might cause a reload. This problem is resolved in Release 12.1(13)E4. (CSCdz39636)
- After Automatic Protection Switching (APS) switchover on OSM-1CHOC12/T1-SI modules, 64 Kbps serial interfaces might flap. This problem is resolved in Release 12.1(13)E4. (CSCdz39636)
- If you configure QSAAL or ILMI virtual circuits (VCs) on a 2-port OC-12 ATM OSM interface, you will not be able to configure AAL5SNAP VCs on that same interface. If you try to do this, the following message will display:

  ```
  00:12:38:%CWANLC_ATM-4-MISMATCH_VCENCAP:ATM9/2:Cannot mix aal5snap & mux
  VCs in same swidb
  ```

  This problem is resolved in Release 12.1(13)E4. (CSCdz62725)
- The **arp** *ip_address mac_address* {**srp-a** | **srp-b**} command does not work on OSM-2OC48/1DPT modules. This problem is resolved in Release 12.1(13)E4. (CSCdw13108)

- With no cable connected, an OSM-4GE-WAN-GBIC module incorrectly display status and protocol as “up.” This problem is resolved in Release 12.1(13)E4. (CSCdz45070)

Resolved OSM Caveats in Release 12.1(13)E3

- Occasionally, the “OIRTWICE” error message displays during OIR of two OSMs. This may happened at boot up or during an RPR+ switchover. This problem is resolved in Release 12.1(13)E3. (CSCdz01886)
- An initial reload of the system may cause the OC-48 DPT/POS modules to reload continuously. This problem is resolved in Release 12.1(13)E3. (CSCdy62569)
- If there is no traffic on PVCs configured for BRE on an OC-12 ATM OSM, the counters for the ATM subinterface will display incorrect information. This problem is resolved in Release 12.1(13)E3. (CSCdy87889)
- An OC-48 POS OSM may reset after a system reload. This problem is resolved in Release 12.1(13)E3. (CSCdz03157)
- After an RPR+ switchover, the OSM-4GE-WAN-GBIC ports fails to forward traffic.

  Workaround: Enter a **shutdown** command followed by a **no shutdown** command. This problem is resolved in Release 12.1(13)E3. (CSCdz39010)
- On an OSM-16OC3-POS-MM module with high-speed traffic running on the ports, the line protocol on the ports may occasionally go down after a supervisor engine RPR+ switchover. This problem is resolved in Release 12.1(13)E3. (CSCdz13392)
- If you configure OAM on a multipoint PVC on an OC-12 ATM OSM, the line protocol on the interface will go up and down sporadically. This problem is resolved in Release 12.1(13)E3. (CSCdz20650)

Resolved OSM Caveats in Release 12.1(13)E1

- Because subinterfaces on the OSM-4GE-WAN module cannot share HSRP group numbers, the 4-port Gigabit Ethernet WAN module supports only 16 HSRP groups per Gigabit Ethernet WAN port. This problem is resolved in Release 12.1(13)E1. (CSCdx38389)
- IGMP snooping does not function over an EoMPLS connection if the connection is made over a POS interface. This problem is resolved in Release 12.1(13)E1. (CSCdw73064)
- If you use a subinterface on the 4-port Gigabit Ethernet WAN OSM to connect a Cisco 7600 series router or Catalyst 6500 series switch Provider Edge to an MPLS core, the VLAN ID on the subinterface cannot be the same as the VLAN ID of the VLAN interface where the EoMPLS route is configured. This problem is resolved in Release 12.1(13)E1. (CSCdv79130, CSCdw61392)
- If multiple OC-12-ATM OSMs with large configurations are installed in a system, you may not be able to boot the OC-12-ATM OSMs simultaneously. This problem is resolved in Release 12.1(13)E1. (CSCdy21621, CSCdy14468)
- In a system with a channelized DS3 OSM installed and more than 10,000 IP routes present, the following error message may be displayed for the channelized DS3 OSM:

  ```
  FIB-3-FIBDISABLE: Fatal error, slot/cpu 4/0: no memory
  ```

  This problem is resolved in Release 12.1(13)E1. (CSCdy19072, CSCdy40632)
- In a system with a large number of Frame Relay subinterfaces configured, some subinterfaces will not be functional after the system switches over from the active route processor to the redundant route processor. This problem is resolved in Release 12.1(13)E1. (CSCdy26531)

- With Ethernet over MPLS, a problem may occur when the label switched path (LSP) for an Ethernet over MPLS VC is changed and a new tunnel label for the new LSP is used. Instead of sending the frame with the new tunnel label, the frame is sent with the old tunnel label. This problem is resolved in Release 12.1(13)E1. (CSCdy34983)
- A mixed configuration of E3s and T3s on an AU-4 fails on OSM-1CHOC12/T3 modules. This problem is resolved in Release 12.1(13)E1. (CSCdy76612)
- The Gigabit Ethernet WAN OSMs stop forwarding packets greater than 12K because of an ASIC problem that causes link errors. This problem is resolved in Release 12.1(13)E1. (CSCdy70722)

Resolved OSM Caveats in Release 12.1(13)E

None.

Release 12.1(12c)E and Rebuilds

- General Caveats, page 262
- FlexWAN Module Caveats, page 267
- OSM Caveats, page 268

General Caveats

- Open General Caveats in Release 12.1(12c)E5, page 262
- Resolved General Caveats in Release 12.1(12c)E5, page 263
- Resolved General Caveats in Release 12.1(12c)E4, page 263
- Resolved General Caveats in Release 12.1(12c)E2, page 264
- Resolved General Caveats in Release 12.1(12c)E1, page 264

Open General Caveats in Release 12.1(12c)E5

- On a Layer 3 EtherChannel, applying an ACL to both the port-channel interface and a member port prevents the ACL from denying traffic correctly.

  Workaround: Remove the ACL from both the port-channel interface and the member port and reapply it only to the port-channel interface. This problem is resolved in Release 12.1(13)E5. (CSCdz56987)
- In a system that has policing configured and a Switch Fabric Module installed, the “AgId” field is reset to zero in the display after an OIR of a Switch Fabric Module, and the counters may not show packets that are policed.

  Workaround: Reapply the policy, or remove and then reconfigure global QoS. This problem is resolved in Release 12.1(13)E. (CSCdy19696)
- If you enter the **do** command under the **interface range** command, Cisco IOS executes the **do** command for each interface in the range. This problem is resolved in Release 12.1(13)E. (CSCdw92111)

- In a system with a Switch Fabric Module installed, the following error message might be displayed when a Switch Fabric Module is reset or powered down if the traffic load is heavy:

  ```
  %CWAN_RP-1-LCLOG_MSG: slot 3/0 Rx SOAP hardware error: source 0x1 deta il 0x0
  ```

  (CSCdx87261)

  Note CSCdx87261 is not seen in later releases.

- With a PFC2 and DFCs, you cannot configure Layer 2 EtherChannels that include interfaces on different DFC-equipped switching modules. You can do the following:
  - Create Layer 3 EtherChannels that include ports on different DFC-equipped switching modules.
  - Create Layer 2 EtherChannels that include ports on a single DFC-equipped switching module.
  - Create Layer 2 EtherChannels that include supervisor engine ports and ports on non-DFC-equipped switching modules.

  Note Layer 2 EtherChannels are formed from ports configured with the **switchport** keyword.

  This problem is resolved in Release 12.1(13)E. (CSCdt27074)

Resolved General Caveats in Release 12.1(12c)E5

- A reload occurs with an "%ALIGN-1-FATAL: Illegal access to a low address" message. There is no crashinfo file. This problem is resolved in Release 12.1(12c)E5. (CSCdz00002)
- A reload occurs when you disable IGMP snooping. This problem is resolved in Release 12.1(12c)E5. (CSCdy89124)
- The **mls ip reflect-threshold**, **mls ip delete-threshold**, and **mls ip install-threshold** commands are not saved in nonvolatile memory. This problem is resolved in Release 12.1(12c)E5. (CSCdy54824)

Resolved General Caveats in Release 12.1(12c)E4

- When multiple switches create a loop that is blocked by STP at the SSG and there is a link failure and recovery on the primary forwarding link between the RLB and the SSG, traffic stops until the MAC address age timer expires. This problem is resolved in Release 12.1(12c)E4. (CSCdy34266)
- Slow replication of conn, sticky, and radius tables occurs when the tables are large and the primary SLB is preempting the secondary in a stateful configuration. This problem is resolved in Release 12.1(12c)E4. (CSCdy60253)
- SLB FWLB traffic from an address behind a firewall going to an address behind a firewall (the same or a different firewall) is routed by the MSFC. This problem is resolved in Release 12.1(12c)E4. (CSCdy49381)
- When the **failaction radius reassign** command has not been entered and the real server fails, IOS-SLB RADIUS Load Balancing incorrectly chooses a different real server to load balance RADIUS interim accounting requests. This problem is resolved in Release 12.1(12c)E4. (CSCdy67824)
- Spurious accesses or a reload might occur if you enter the **aaa authorization auth-proxy** command. This problem is resolved in Release 12.1(12c)E4. (CSCdy68457)
- With MPLS VPN configured, a reload might occur with an %MSFC2-3-MISTRAL_BAD_PAK message. This problem is resolved in Release 12.1(12c)E4. (CSCdy43996)

- With Supervisor Engine 2, multicast packets that set the router alert option, like IGMP general queries and membership reports, might not be handled properly, which might disrupt IGMP client connectivity. This problem is resolved in Release 12.1(12c)E4. (CSCdy84078)
- With Supervisor Engine 2, packet loss might occur for a few seconds after routing protocol multicast packets are received. This problem is resolved in Release 12.1(12c)E4. (CSCdy58383)
- If the shared tree and the shortest path tree (SPT) diverge because of a Reverse Path Forwarding (RPF) change on the shared tree (normally triggered by a restoration of a failed link), the SPT is pruned. A join to restore the traffic flow immediately follows the prune, which might interrupt traffic briefly. This problem is resolved in Release 12.1(12c)E4. (CSCdu74664)
- If you configure an active member port of an EtherChannel as a SPAN source port, the port goes into the suspended state and does not pass any traffic. In Release 12.1(12c)E4, you cannot configure an active member port of an EtherChannel as a SPAN source port. (CSCdx81246)

Resolved General Caveats in Release 12.1(12c)E2

- Switchover to the redundant supervisor engine and MSFC incorrectly does not occur when excessive interrupts on the supervisor engine cause the MSFC to reload. This problem is resolved in Release 12.1(12c)E2. (CSCdx43539)
- A reload caused by excessive interrupts might fail and CPU-6-MONITOR-SP-NOT-HEARD messages are displayed. This problem is resolved in Release 12.1(12c)E2. (CSCdy27356)
- With heavy traffic, a SYS-3-NULLIDB traceback message might be displayed and crypto tunnels might go down. This problem is resolved in Release 12.1(12c)E2. (CSCdw01724)
- Spurious accesses occur when you clear one of the VPNv4 Multicast Border Gateway Protocol (MBGP) members of a Multi-Protocol Border Gateway Protocol (MP-BGP) peer group. This problem is resolved in Release 12.1(12c)E2. (CSCdw03988)
- Nonmaskable interrupts (NMIs) might cause a Supervisor Engine 1 to reload, and then the reload might fail. This problem is resolved in Release 12.1(12c)E2. (CSCdy25902)
- After primary load-balancer (SLB or FWLB) failure and recovery, if no SLB connection objects were bound to the sticky table entries on the backup load-balancer, the primary load-balancer sticky table might be incomplete. This problem is resolved in Release 12.1(12c)E2. (CSCdy28514)
- Duplicate RMON alarms are sent when there is more than one **snmp-server host** command in the configuration. This problem is resolved in Release 12.1(12c)E2. (CSCdx89905)
- If both IOS Server Load Balancing (SLB) and IOS Firewall Load Balancing (FWLB) are configured on the same router, ICMP packets that need to be firewall load balanced are routed by SLB instead. This problem is resolved in Release 12.1(12c)E2. (CSCdy18588)
- The **show module** command always displays the state of a redundant PFC as **other**. This problem is resolved in Release 12.1(12c)E2. (CSCdy19682)

Resolved General Caveats in Release 12.1(12c)E1

- A multilink PPP bundle might forward traffic intermittently. This problem is resolved in Release 12.1(12c)E1. (CSCin03257)
- To avoid a reload, do not shut down any interfaces while another user is displaying the output from the **show ip pim neighbor** command. This problem is resolved in Release 12.1(12c)E1. (CSCdx25551)
- A Gigabit Ethernet EtherChannel formed with DFC-supported ports and nonDFC-supported ports and configured not to use PAgP may stop passing traffic if you reset or OIR one of the Gigabit Ethernet switching modules. This problem is resolved in Release 12.1(12c)E1. (CSCdx00390)

- When an (S,G) entry with the T flag set transitions to an (S,G,R) entry an (S,G) RP-bit prune is sent towards the source instead of towards the RP. This problem is resolved in Release 12.1(12c)E1. (CSCdw95442)
- A reload might occur when you enter the **show ip mroute** command. This problem is resolved in Release 12.1(12c)E1. (CSCdw20251)
- The **distribute-list** *list_number* **out** *protocol protocol_number* command does not work. This problem is resolved in Release 12.1(12c)E1. (CSCdu52717)
- VLANs in the 1002 to 1005 range are disabled by default in Catalyst software. In the Cisco IOS images for the Catalyst 6500 series switches and Cisco 7600 Series Routers, the VLANs are in the forwarding state by default. This default discrepancy might cause a problem in a situation where a system running Release 12.1(8a)E3 or later on the supervisor engine and the MSFC is connected through an 802.1 Q tunnel to a system running Catalyst software. If the system running Cisco IOS software sends BPDUs for reserved VLANs in the 1002 to 1005 range, the system running Catalyst software drops these BPDUs and increments the rxTotalDrop counter. This problem is resolved in Release 12.1(12c)E1. (CSCdx28347)
- With Supervisor Engine 2, any access to an invalid address in the valid I/O address space can suspend all operation. This problem is resolved in Release 12.1(12c)E1. (CSCdx81901)
- A failure in communication between the MSFC and supervisor engine causes the MSFC to be reset by an internal message from the supervisor engine. This problem is resolved in Release 12.1(12)E1. (CSCdx38960)
- The drop counters on Gigabit Ethernet interfaces might incorrectly increment excessively, even during low traffic conditions. No data is actually dropped. This problem is resolved in Release 12.1(12c)E1. (CSCdv86024)
- Under some circumstances, the router might close an SSH session if a high volume of debug information is flowing through the connection. This problem is resolved in Release 12.1(12c)E1. (CSCdv09709)
- A router configured with Border Gateway Protocol (BGP) **neighbor** *address* or **neighbor ibgp peer-group** *name* **nlri unicast multicast** commands does not automatically translate the **no auto-summary** command into the multicast address family. This problem is resolved in Release 12.1(12c)E1. (CSCdy04712)
- When the MPLS labeled path for a a prefix is down and an unlabeled backup path takes over, the PFC2 is not updated to use the unlabeled backup path. This problem is resolved in Release 12.1(12c)E1. (CSCdx90903)
- BGP prereorganization conversion at boot time does not work properly for connected or static routes in address family IPv4 multicast. This problem is resolved in Release 12.1(12c)E1. (CSCdw39926)
- The MSFC incorrectly updates the Reverse Path Forwarding (RPF) neighbor of an (S,G) entry, which might cause the MSFC to send (S,G) Join/Prune messages and create incorrect multicast route entries. This problem is resolved in Release 12.1(12c)E1. (CSCdx61141)
- In a network where network devices are using different software releases, the MSFC might freeze in the LOADING state after an area boundary router (ABR) sends OSPF link-state advertisements (LSAs) that have an illegal mask to a neighboring network device running a newer software release. This problem is resolved in Release 12.1(12c)E1. (CSCdx42686)
- In dispatch mode, IOS SLB might not route server-bound or firewall-bound IP trailer fragments to the correct real server or firewall. This problem is resolved in Release 12.1(12c)E1. (CSCdx75359)
- When approximately 500 static NAT entries are configured, and the **mls aclmerge algorithm odm** command is configured, a reload might occur if you enter an **ip nat outside** command for an active interface. This problem is resolved in Release 12.1(12c)E1. (CSCdx74455)

- The MSFC might reload after receiving OSPF link-state advertisements (LSAs) that have an illegal mask. This problem is resolved in Release 12.1(12c)E1. (CSCdx70216)
- An extremely complex ACL configuration might cause “idbman_get_port_idb: slot out of range for slot” messages. This problem is resolved in Release 12.1(12c)E1. (CSCdx68009)
- The TestIpFibShortcut diagnostic fails intermittently. This problem is resolved in Release 12.1(12c)E1. (CSCdx53670)
- DFC-equipped switching modules might not initialize properly after a reload. This problem is resolved in Release 12.1(12c)E1. (CSCdx52003)
- Heavy VPN traffic might increase MSFC CPU utilization and cause OSPF adjacencies to be lost. This problem is resolved in Release 12.1(12c)E1. (CSCdx47514)
- You cannot configure more than 16 HSRP groups per port on subinterfaces configured on OSM-4GE-WAN ports. This problem is resolved in Release 12.1(12c)E1. (CSCdx38389)
- Some packets might be dropped on a Fast Ethernet port that is sending traffic to a Content Switching Module (CSM) configured to perform Network Address Translation (NAT). This problem is resolved in Release 12.1(12c)E1. (CSCdx38234)
- IPC-SP-5-WATERMARK messages indicating that many messages are pending might be displayed continuously. There are no messages pending; this is a cosmetic defect with the messages pending counter. This problem is resolved in Release 12.1(12c)E1. (CSCdw74873)
- A reload might occur after IPC-5-LIMIT messages are displayed. This problem is resolved in Release 12.1(12c)E1. (CSCdv53846)
- A VACL configured with the capture option incorrectly captures traffic that should be denied by a Cisco IOS ACL. This problem is resolved in Release 12.1(12c)E1. (CSCdu61309)
- In a redundant configuration, after you receive LYRA-SP-2-PARITY_ERR messages, switchover to the standby Supervisor Engine 2 did not occur. This problem is resolved in Release 12.1(12c)E1. (CSCdx44052)
- With 7,000 NAT entries and 3 kpps of NAT traffic, MSFC CPU utilization is 100 percent. This problem is resolved in Release 12.1(12c)E1. (CSCdx40232)
- After a reload that is caused by a fault, a crashinfo file might not exist. This problem is resolved in Release 12.1(12c)E1. (CSCdx38379)
- If you install three or more Content Services Gateway (CSG) modules in the same chassis, a reload occurs. This problem is resolved in Release 12.1(12c)E1. (CSCdw77156)
- Packets between fabric-enabled modules can be forwarded from one module to another using either 8-Gigabit Ethernet fabric interface or the 16-Gigabit Ethernet backplane bus.

  With less than three fabric-enabled modules installed, replicated multicast packets are occasionally sent over the fabric as well as the backplane bus, causing ports to receive twice as many packets as were generated. This problem is resolved in Release 12.1(12c)E1. (CSCdw82490)
- To avoid unreliable operation, do not enter the **do** command in EXEC mode. This problem is resolved in Release 12.1(12c)E1. (CSCdx02925)

- Only the 4-port Gigabit Ethernet WAN module (OSM-4GE-WAN) supports Layer 3 trunks. Configuring a subinterface on a LAN port might cause a reload. This problem is resolved in Release 12.1(12c)E1. (CSCdx24623)
- If you configure more than 16 HSRP group numbers for different VLAN interfaces in a system with a PFC1, the following error message is displayed:

  ```
  More than 16 standby groups not supported in this platform.
  ```

  This problem is resolved in Release 12.1(12c)E1. (CSCdx32496)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(12c)E5, page 267
- Resolved FlexWAN Module Caveats in Release 12.1(12c)E5, page 268
- Resolved FlexWAN Module Caveats in Release 12.1(12c)E4, page 268
- Resolved FlexWAN Module Caveats in Release 12.1(12c)E2, page 268
- Resolved FlexWAN Module Caveats in Release 12.1(12c)E1, page 268

Open FlexWAN Module Caveats in Release 12.1(12c)E5

- During a PVC discovery test on an ATM port adapter, the MSFC hangs while trying to create a subinterface for the PVC discovery. This problem is resolved in Release 12.1(14)E. (CSCdy71452)
- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan***slot_number/port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module **crashinfo** file with the **copy cwan***slot_number/port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)
- If you enable and disable MMLS on ATM subinterfaces with a combination of point-to-point and multipoint subinterfaces, multicast shortcuts may not be created for multipoint connections, or in some cases multicast traffic may fail. (CSCdr01409)

  Note CSCdr01409 is not seen in later releases.

- In a system installed with a FlexWAN and a PA-A3 ATM port adapter, the ATM interface may stay down after you enter a **shutdown** command followed immediately by a **no shutdown** command.

  Workaround: After you enter the **shutdown** command on the interface, wait for 1 minute before entering the **no shutdown** command. This problem is resolved in Release 12.1(20)E. (CSCdy23751, CSCdw65799)
- If the cable is removed and replaced on a FlexWAN module with an ATM port adapter installed, the line protocol shows as UP but no switched virtual circuits (SVCs) are created. This behavior occurs if traffic is running and 200 or more SVCs have been configured.

  Workaround: Enter a **shutdown** command followed by **no shutdown** command on the affected interface. (CSCdy24309)

  Note CSCdy24309 is not seen in later releases.

- Because of an inter-process communication failure on the MSFC, the supervisor engine might reset after SVC traffic is forwarded on a FlexWAN ATM port adapter. This problem is resolved in Release 12.1(13)E1. (CSCdy18390)
- After an OIR, a FlexWAN module may fail to save a crash-information file after a reset if it has a Packet-over-SONET (POS) port adapter with 500 Frame Relay point-to-point DLCIs in Bay 0 and an ATM port adapter with 500 point-to-point operation, administration, and maintenance PVCs in Bay 1. This problem is resolved in Release 12.1(13)E3. (CSCdy18458, CSCdy09631)

Resolved FlexWAN Module Caveats in Release 12.1(12c)E5

None.

Resolved FlexWAN Module Caveats in Release 12.1(12c)E4

- After you move multilink members from one FlexWAN module to another, traffic does not pass through the multilink interface. This problem is resolved in Release 12.1(12c)E4. (CSCdy24019)
- Some FlexWAN multilink interfaces might stop passing traffic following a reload. This problem is resolved in Release 12.1(12c)E4. (CSCin12517)

Resolved FlexWAN Module Caveats in Release 12.1(12c)E2

- An ALIGN-1-FATAL:RSP_update_linecard_vc_blt_state message might be displayed, followed by a reload. This problem is resolved in Release 12.1(12c)E2. (CSCdy17228)

Resolved FlexWAN Module Caveats in Release 12.1(12c)E1

None.

OSM Caveats

- Open OSM Caveats in Release 12.1(12c)E5, page 268
- Resolved OSM Caveats in Release 12.1(12c)E5, page 269
- Resolved OSM Caveats in Release 12.1(12c)E4, page 270
- Resolved OSM Caveats in Release 12.1(12c)E2, page 270
- Resolved OSM Caveats in Release 12.1(12c)E1, page 270

Open OSM Caveats in Release 12.1(12c)E5

- IGMP snooping does not function over an EoMPLS connection if the connection is made over a POS interface. There is no workaround. This problem is resolved in Release 12.1(13)E1. (CSCdw73064)
- If you use a subinterface on the 4-port Gigabit Ethernet WAN OSM to connect a Cisco 7600 series router or Catalyst 6500 series switch Provider Edge to an MPLS core, the VLAN ID on the subinterface must not coincide with the VLAN ID of the VLAN interface where the EoMPLS route is configured.

  Workaround: Assign a different VLAN ID for the subinterface. This problem is resolved in Release 12.1(13)E1. (CSCdv79130, CSCdw61392)

- In an MPLS-VPN topology where a Catalyst 6500 series switch or Cisco7600 Internet Router is functioning as a provider router, the following informational error messages might be displayed:

```
*Jul  1 18:25:23.709: %TFIB-7-SCANSABORTED: TFIB scan not completing.  MAC string
updated.
*Jul  1 18:25:25.285: %TFIB-DFC8-7-SCANSABORTED: TFIB scan not completing.  MAC string
updated.
*Jul  1 18:26:24.049: %TFIB-7-SCANSABORTED: TFIB scan not completing.  MAC string
updated.
*Jul  1 18:27:23.945: %TFIB-7-SCANSABORTED: TFIB scan not completing.  MAC string
updated.
*Jul  1 18:27:24.949: %TFIB-SP-7-SCANSABORTED: TFIB scan not completing.  MAC string
updated.
```

  These messages continue to be displayed until you reload the system. After a steady traffic rate is reached, the error messages should stop. While these messages are displayed, route processor and switch processor CPU utilization also increases to 100 percent because a background process is attempting to converge the network. (CSCdy21998)

  Note CSCdy21998 is not seen in later releases.

- After an OIR of a FlexWAN or OSM, the following error message might be displayed if the route processor is busy and CPU utilization is more than 60 percent:

```
%FIB-3-FIBDISABLE: Fatal error, slot/cpu 10/1: No window message, LC to RP IPC is
non-operational
```

  When this condition occurs, traffic forwarding stops on the affected module.

  Workaround: Reset the affected module one more time, which may resolve the problem. (CSCdx75137)

  Note CSCdx75137 is not seen in later releases.

- If multiple OC-12-ATM OSMs with large configurations are installed in a system, you may not be able to boot the OC-12-ATM OSMs simultaneously. This problem is resolved in Release 12.1(13)E1. (CSCdy21621, CSCdy14468)
- In a system with a channelized DS3 OSM installed and more than 10,000 IP routes present, the following error message may be displayed for the channelized DS3 OSM:

```
FIB-3-FIBDISABLE: Fatal error, slot/cpu 4/0: no memory
```

  Workaround: Upgrade the memory on the channelized DS3 OSM from 64 MB to 128 MB. This problem is resolved in Release 12.1(13)E1. (CSCdy19072, CSCdy40632)
- In a system with a large number of Frame Relay subinterfaces configured, some subinterfaces will not be functional after the system switches over from the active route processor to the redundant route processor.

  Workaround: Enter a **shutdown** command followed by a **no shutdown** command on the main interface. This problem is resolved in Release 12.1(13)E1. (CSCdy26531)

Resolved OSM Caveats in Release 12.1(12c)E5

None.

Resolved OSM Caveats in Release 12.1(12c)E4

None.

Resolved OSM Caveats in Release 12.1(12c)E2

None.

Resolved OSM Caveats in Release 12.1(12c)E1

- Because subinterfaces on the OSM-4GE-WAN module cannot share HSRP group numbers, the 4-port Gigabit Ethernet WAN module supports only 16 HSRP groups per Gigabit Ethernet WAN port. This problem is resolved in Release 12.1(12c)E1. (CSCdx38389)
- In a configuration where global virtual routing and forwarding instance (VRF) routes are configured on a 4-port Gigabit Ethernet WAN OSM, when you ping a global IP address from a customer-edge device within a VPN, the ping fails. This failure occurs because a VRF-forwarding Gigabit Ethernet interface can resolve ARPs in the VRF ARP table, but it cannot be in the default ARP table. This problem is resolved in Release 12.1(12c)E1. (CSCdw74766, CSCin04666)
- Transmission of IP packets between MPLS clouds over Generic Routing Encapsulation GRE tunnels is not supported. This problem is resolved in Release 12.1(12c)E1. (CSCdw62753)
- PFC2-based QoS is supported on all the OSMs but has not been fully tested on the 2-port OC-12 ATM OSMs and the channelized OSMs. The PFC2 QoS CLI is not blocked for these modules, but we do not recommend that you configure PFC2-based QoS until testing has been completed. This problem is resolved in Release 12.1(12c)E1. (CSCdw84716)

Release 12.1(11b)E and Rebuilds

Note

- All images in Release 12.1(11b)E2 are deferred.
- All caveats resolved in Release 12.1(8a)EX are resolved in Release 12.1(11b)E. Refer to these URLs:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/121_8aex/ol_1923.htm#287923

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/121_8aex/ol_1923.htm#287822

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/121_8aex/ol_1923.htm#242341

- General Caveats, page 270
- FlexWAN Module Caveats, page 278
- OSM Caveats, page 279

General Caveats

- Open Caveats in Release 12.1(11b)E14, page 271
- Resolved Caveats in Release 12.1(11b)E14, page 272
- Resolved Caveats in Release 12.1(11b)E12, page 273
- Resolved Caveats in Release 12.1(11b)E11, page 273

- Resolved Caveats in Release 12.1(11b)E7, page 274
- Resolved Caveats in Release 12.1(11b)E4, page 274
- Resolved Caveats in Release 12.1(11b)E3, page 275
- Resolved Caveats in Release 12.1(11b)E2, page 275
- Resolved Caveats in Release 12.1(11b)E1, page 276
- Resolved Caveats in Release 12.1(11b)E, page 277

Open Caveats in Release 12.1(11b)E14

- On a Layer 3 EtherChannel, applying an ACL to both the port-channel interface and a member port prevents the ACL from denying traffic correctly.

  Workaround: Remove the ACL from both the port-channel interface and the member port and reapply it only to the port-channel interface. This problem is resolved in Release 12.1(13)E5. (CSCdz56987)

- If both IOS Server Load Balancing (SLB) and IOS Firewall Load Balancing (FWLB) are configured on the same router, ICMP packets that need to be firewall load balanced are routed by SLB instead. This problem is resolved in Release 12.1(12c)E2. (CSCdy18588)

- Packets between fabric-enabled modules can be forwarded from one module to another using either 8-Gigabit Ethernet fabric interface or the 16-Gigabit Ethernet backplane bus. In a system where less than three fabric-enabled modules are installed, replicated multicast packets are occasionally sent over the fabric as well as the backplane bus, causing ports to receive twice as many packets as were generated.

  Workaround: Override the default bus mode by entering the **fabric switching-mode allow truncated threshold 1** command. This problem is resolved in Release 12.1(12c)E1. (CSCdw82490)

- To avoid unreliable operation, do not enter the **do** command in EXEC mode.

  Workaround: Turn the switch off and back on again. This problem is resolved in Release 12.1(12c)E1. (CSCdx02925)

- If you enter the **do** command under the **interface range** command, Cisco IOS executes the **do** command for each interface in the range. This problem is resolved in Release 12.1(13)E. (CSCdw92111)

- Catalyst 6500 series switches and Cisco 7600 Series Routers support Layer 3 trunks only on the 4-port Gigabit Ethernet WAN module (OSM-4GE-WAN). If you configure a subinterface on a LAN port, a reload might occur.

  Workaround: Do not configure subinterfaces on LAN ports. Catalyst 6500 series switches and Cisco 7600 Series Routers support Layer 2 trunks and Layer 3 VLAN interfaces, which provide equivalent capabilities for LAN ports. This problem is resolved in Release 12.1(12c)E1. (CSCdx24623)

- With a PFC2 and DFCs, you cannot configure Layer 2 EtherChannels that include interfaces on different DFC-equipped switching modules. You can do the following:
  - Create Layer 3 EtherChannels that include ports on different DFC-equipped switching modules.
  - Create Layer 2 EtherChannels that include ports on a single DFC-equipped switching module.
  - Create Layer 2 EtherChannels that include supervisor engine ports and ports on non-DFC-equipped switching modules.

  Note Layer 2 EtherChannels are formed from ports configured with the **switchport** keyword.

  This problem is resolved in Release 12.1(13)E. (CSCdt27074)

Resolved Caveats in Release 12.1(11b)E14

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in Release 12.1(11b)E14. (CSCed27956, CSCed38527)
- In rare situations, an MSFC2 might freeze when it can receive control traffic from the supervisor engine, but it cannot send it. This problem is resolved in Release 12.1(11b)E14. (CSCdy15598)
- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

  This problem is resolved in Release 12.1(11b)E14. (CSCdx40184, CSCdx76632, CSCea46342, CSCeb78836, CSCec76776, CSCed28873, CSCin56408)

- There might be OSPF neighbor drops and HSRP flaps when QoS is enabled on a Supervisor Engine 1 and MSFC2. This problem is resolved in Release 12.1(11b)E14. (CSCeb55271)

Resolved Caveats in Release 12.1(11b)E12

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.1(11b)E12. (CSCdu53656)

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.1(11b)E12. (CSCea28131)

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

  This problem is resolved in Release 12.1(11b)E12. (CSCea02355)

Resolved Caveats in Release 12.1(11b)E11

- Cisco devices which run IOS and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default. The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at this URL:

  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

  This problem is resolved in Release 12.1(11b)E11. (CSCdz60229)

Resolved Caveats in Release 12.1(11b)E7

- With Supervisor Engine 2, any access to an invalid address in the valid I/O address space can suspend all operation. This problem is resolved in Release 12.1(11b)E7. (CSCdx81901)
- Switchover to the redundant supervisor engine and MSFC does not occur following a problem on the MSFC that should cause a switchover. This problem is resolved in Release 12.1(11b)E7. (CSCdx43539)
- A reload caused by excessive interrupts might fail, with CPU-6-MONITOR-SP-NOT-HEARD messages displayed. This problem is resolved in Release 12.1(11b)E7. (CSCdy27356)
- With heavy traffic, a SYS-3-NULLIDB traceback message might be displayed and crypto tunnels might go down. This problem is resolved in Release 12.1(11b)E7. (CSCdw01724)
- Nonmaskable interrupts (NMIs) might cause a Supervisor Engine 1 to reload and the reload might fail. This problem is resolved in Release 12.1(11b)E7. (CSCdy25902)
- With Release 12.1(11b)E, Release 12.1(11b)E1, Release 12.1(11b)E2, Release 12.1(11b)E3, Release 12.1(11b)E4, and Release 12.1(12c)E1, the IPSEC prefragmentation feature is enabled by default with the tunnel interface MTU size set to 1520 bytes. Other releases use 1576 bytes. This problem is resolved in Release 12.1(11b)E7. (CSCdy03649)
- If you install three or more Content Services Gateway (CSG) modules in the same chassis, a reload occurs. This problem is resolved in Release 12.1(11b)E7. (CSCdw77156)
- Nonmaskable interrupts (NMIs) might cause a Supervisor Engine 1 to reload, and then the reload might fail. This problem is resolved in Release 12.1(11b)E7. (CSCdy25902)

Resolved Caveats in Release 12.1(11b)E4

- A multilink PPP bundle might forward traffic intermittently. This problem is resolved in Release 12.1(11b)E4. (CSCdx48611)
- VLANs in the 1002 to 1005 range are disabled by default in Catalyst software. In the Cisco IOS images for the Catalyst 6500 series switches and Cisco 7600 Series Routers, the VLANs are in the forwarding state by default. This default discrepancy might cause a problem in a situation where a system running Release 12.1(8a)E3 or later on the supervisor engine and the MSFC is connected through an 802.1 Q tunnel to a system running Catalyst software. If the system running Cisco IOS software sends BPDUs for reserved VLANs in the 1002 to 1005 range, the system running Catalyst software drops these BPDUs and increments the rxTotalDrop counter. This problem is resolved in Release 12.1(11b)E4. (CSCdx28347)
- When the VLAN-bridge protocol is used, VLAN bridge BPDUs are not sent even though the interface BPDU counters indicate that BPDUs are sent. This problem is resolved in Release 12.1(11b)E4. (CSCdw80500)
- The following error message displays when an SNMP cardTable MIB walk is performed:

  ```
  c6k_pwr_get_fru_present(): can't find fru_info for fru type 6, #66
  ```

  This problem is resolved in Release 12.1(11b)E4. (CSCdx41473)
- When you enter the **no ip routing** command followed by the **ip routing** command, the following error message appears:

  ```
  A%FIB-4-FIBCBLK
  ```

  This problem is resolved in Release 12.1(11b)E4. (CSCin09681)

Resolved Caveats in Release 12.1(11b)E3

- The **distribute-list** *list_number* **out** *protocol protocol_number* command does not work. This problem is resolved in Release 12.1(11b)E3. (CSCdu52717)
- A sequencing problem results when there are NAT ACL configurations and static NAT entries in the startup configuration at bootup. The problem results in incorrect entries being programmed into the ternary content addressable memory (TCAM). This problem is resolved in Release 12.1(11b)E3. (CSCdx35689)
- A malfunctioning DC-to-DC convertor on the WS-X6816 module affects the Ethernet Out of Band Channel (EOBC) channel and causes the active supervisor engine to lose communication with other modules in the system. This problem is resolved in Release 12.1(11b)E3. (CSCdx34821)
- A failure in communication between the MSFC and supervisor engine causes the MSFC to be reset by an internal message from the supervisor engine. This problem is resolved in Release 12.1(11b)E3. (CSCdx38960)
- When two CSMs are present in a Catalyst 6500 series switch, EtherChannels cannot be successfully created. This problem eventually causes the switch to reset. This problem is resolved in Release 12.1(11b)E3. (CSCdx13346)
- A route map containing the **match nlri unicast multicast** clause is broken into two route maps, one with the original route map tag and the another with an **_mcast** extended tag. This translation is either automatically done or user-initiated if **bgp upgrade-cli** is available. If the original route-map contained a **match community** *community name* or **match extcommunity** *extended community-list number* entry, the MSFC may reload if the **write terminal**, **show running-config**, or **show route-map** command is entered after the original route-map is deleted. This problem is resolved in Release 12.1(11b)E3. (CSCdx46554)

Resolved Caveats in Release 12.1(11b)E2

Note All images in Release 12.1(11b)E2 are deferred.

- In a PFC2/MSFC2 system with a fabric-enabled 48-port 10/100 Mbps RJ-45 module and a fabric-enabled 16-port 1000 Mbps GBIC module installed, when traffic enters the RJ-45 and exits through the GBIC module, or vice versa, dCEF forwarding is not enabled on the ingress module and traffic is dropped at the ingress port. This problem is resolved in Release 12.1(11b)E2. (CSCdw55635)
- The **show mls aging** command does not show the correct default aging values for long and normal aging. This problem is resolved in Release 12.1(11b)E2. (CSCdx14798)
- The **show mls ip** command displays incorrect age of NetFlow entries. This problem is resolved in Release 12.1(11b)E2. (CSCdx14827)
- The supervisor engine reloads when a **write terminal** command is entered. This problem is resolved in Release 12.1(11b)E2. (CSCdw83512)
- A packet encapsulation error occurs in Data-Link Switching (DLSw). This problem is resolved in Release 12.1(11b)E2. (CSCdx20546)
- With loose Unicast RPF configured on the MSFC, traffic that should be dropped is still forwarded through the MSFC. This problem is resolved in Release 12.1(11b)E2. (CSCdw92775)
- IP connectivity to the supervisor engine Gigabit Ethernet ports does not work in Release 12.1(11b)E. This problem is resolved in Release 12.1(11b)E2. (CSCdx04363)

- Because of a lack of IPC buffer space, a system with a Supervisor Engine1 and an MSFC2 running Release 12.1(8b)E8 may reload when InterCard Communication (ICC) messages are waiting in the queue. Before the system reloads, messages similar to these may appear:

```
%ICC-SP-5-WATERMARK:5988 pkts for class L3-MGR are waiting to be processed
%IPC-SP-3-NOBUFF:The main IPC message header cache has emptied
```

  This problem is resolved in Release 12.1(11b)E2. (CSCdw53279, CSCdx05096)

- A system with a Supervisor Engine 1 and either an MFCS1 or MSFC2 may reload when the number of buffers available is exhausted. This problem is resolved in Release 12.1(11b)E2. (CSCdx16248)

Resolved Caveats in Release 12.1(11b)E1

- With Supervisor Engine 2, IOS Server Load Balancing (SLB) does not forward fragmented packets in accordance with the RADIUS Load Balancing framed-IP sticky database. This problem only affects trailer-fragmented IP packets sourced by a subscriber whose IP address is in the framed-IP sticky database when the **ip slb route** command is entered. This problem is resolved in Release 12.1(11b)E1. (CSCdw86527)
- The IOS Server Load Balancing **ip slb natpool** command is not accepted upon reload if configuration of the initial allocation or maximum allocation of client NAT address entities is configured. This allocation is configured using the **entries** keyword.

  Workaround: Enter the **ip slb natpool** command without the **entries** keyword. This problem is resolved in Release 12.1(11b)E1. (CSCdw88469)
- With a Supervisor Engine 2, IOS Firewall Load Balancing (FWLB) does not install hardware shortcuts in the firewall-to-host direction. Functionality works correctly, but performance is affected. This problem is resolved in Release 12.1(11b)E1. (CSCdx01014)
- Supervisor Engine 2 might incorrectly show that an ACL entry has been made in the TCAM, when actually there are insufficient TCAM resources available, as indicated by TCAM entry-capacity-exceeded messages. This problem is resolved in Release 12.1(11b)E1. (CSCdw91641)
- With IP or IPX ACLs configured on an interface, any incoming IPX packets with source and destination network numbers set to zero might get dropped on that interface. This problem is resolved in Release 12.1(11b)E1. (CSCdw76549)
- The **mls aging fast** command has no effect. This problem is resolved in Release 12.1(11b)E1. (CSCdw66953)
- MAC address entries on DFCs do not age out. This problem is resolved in Release 12.1(11b)E1. (CSCdw76397)
- If a port is configured as a Layer 2 port with the **switchport** command when the switch boots and is later configured as a Layer 3 port by entering the **no switchport** command, the **show ip interface brief** command displays the port as having an invalid configuration until you enter an **ip address** command or a **no ip address** command. If the invalid configuration is not cleared before the switch is rebooted, the interface is returned to defaults. This problem is resolved in Release 12.1(11b)E1. (CSCdw77676)
- When configured with the **diagnostic level complete** command and with complex VACLs, a switch might fail the diagnostics because the VACLs interfere with the diagnostics. This problem is resolved in Release 12.1(11b)E1. (CSCdw81297)

- The **show module** command incorrectly displays the WS-SVC-CSG-1 Content Services Gateway module as a WS-X6066-SLB-APC Content Switching Module. This problem is resolved in Release 12.1(11b)E1. (CSCdw94918)
- EoMPLS on Flexwan does not work. This problem is resolved in Release 12.1(11b)E1. (CSCin05155)

Resolved Caveats in Release 12.1(11b)E

- If you delete a large number of routes (for example, 150,000), and then add a number of routes (for example, 800), traffic is not switched to the new routes. This problem is resolved in Release 12.1(11b)E. (CSCdv58619, CSCeb16290)
- A multicast output interface might be added to the output interface list more than once. This problem is resolved in Release 12.1(11b)E. (CSCdw54615)
- Layer 3 multicast switching in hardware does not support multicast traffic through interfaces configured with secondary ip subnets. This problem is resolved in Release 12.1(11b)E. (CSCdu71914)
- The **mls ip multicast stub command** does not support secondary ip subnets. This problem is resolved in Release 12.1(11b)E. (CSCdu69367)
- Some malformed IGMP packets can loop through the system causing high CPU utilization. This problem is resolved in Release 12.1(11b)E. (CSCdw41220)
- With a PFC2 and DFCs, do not configure SPAN sessions that include interfaces on fabric-enabled switching modules. This problem is resolved in Release 12.1(11b)E. (CSCds02430)
- PIM sparse mode for the Auto-RP groups might not set the L flag for the RP-discovery group. This problem is resolved in Release 12.1(11b)E. (CSCdr51872, CSCdw13674)
- You can use only the outbound route map to set the next hop for BGP route reflectors and not the **nexthop-self** command. This problem is resolved in Release 12.1(11b)E. (CSCdt84706)
- After a system reset, the Layer 2 global aging timer value is reset to the default value of 300 seconds even though the start-up configuration has the correct values. This problem is resolved in Release 12.1(11b)E. (CSCdv21825)
- In a system with Supervisor Engine 1/MSFC1, individual Layer 2 aging commands for each VLAN might be present in the configuration file although only global Layer 2 aging has been configured. This problem is resolved in Release 12.1(11b)E. (CSCdv21083)
- Configuring protocol filtering on an interface to block IPX, AppleTalk, and other protocols also blocks egress IP and IPX traffic (ingress IP and IPX traffic is not affected). This problem is resolved in Release 12.1(11b)E. (CSCdv23611)
- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) time stamp for the Flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor engine or a PCMCIA card from slave-slot0 when the applications are performing Flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- If you enter an invalid interface range for the SPAN sources or destinations, the SPAN feature may not work correctly and the system might reset. Changing the configuration to reflect a valid interface range corrects this problem. This problem is resolved in Release 12.1(11b)E. (CSCdv07079)
- Configuring more than 64 destination interfaces for one monitor session might cause an incorrect SPAN configuration and a system reset. This problem is resolved in Release 12.1(11b)E. (CSCdv07321)

- Jumbo frame support is incompatible with the IS-IS routing protocol. Leave the MTU size at the default value on any interface where IS-IS provides routing. This problem is resolved in Release 12.1(11b)E. (CSCdu09773, CSCdu48660)
- After you have entered a complete Cisco Appliance Services Architecture (CASA) configuration, a system running 12.1(8a)E4 or later might reload when it receives an update from a Local Director. The specific triggering events might be an interface joining the IGMP group used by a Local Director or configuration of an active forwarding agent by entry of the CASA control address with the forwarding-agent command. This problem is resolved in Release 12.1(11b)E. (CSCdv83097)
- Partial component failures are not reported and do not trigger switchover in redundant supervisor engine configurations. This problem is resolved in Release 12.1(11b)E. (CSCdw31630)
- If a system running Release 12.1(8b)E7 is used in a Server Load Balancing configuration, this error message may occur:

  ```
  Jan 13 19:17:08 MET: %ICC-5-WATERMARK: 1123 pkts for class L3-MGMT are waiting t o be
  processed
  ```

  This problem is resolved in Release 12.1(11b)E. (CSCdw45465)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(11b)E14, page 278
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E14, page 278
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E12, page 278
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E11, page 279
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E4, page 279
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E3, page 279
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E2, page 279
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E1, page 279
- Resolved FlexWAN Module Caveats in Release 12.1(11b)E, page 279

Open FlexWAN Module Caveats in Release 12.1(11b)E14

- On FlexWAN ports, an EoMPLS VC stays up when the VLAN interface is down. (CSCdv69982)
- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan***slot_number*/*port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module **crashinfo** file with the **copy cwan***slot_number*/*port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)

Resolved FlexWAN Module Caveats in Release 12.1(11b)E14

None.

Resolved FlexWAN Module Caveats in Release 12.1(11b)E12

None.

Resolved FlexWAN Module Caveats in Release 12.1(11b)E11

None.

Resolved FlexWAN Module Caveats in Release 12.1(11b)E4

- Multilink bundles may go down intermittently. This problem is resolved in Release 12.1(11b)E4. (CSCdx47373)
- The "packets in" counters for multilinks show twice the number of packets actually received. This problem is resolved in Release 12.1(11b)E4. (CSCin03266)
- After a supervisor engine switchover and reload of a PA-POS-OC3SMI, the remote POS module experiences an increase in new pointer (NEWPTR) errors. This problem is resolved in Release 12.1(11b)E4. (CSCdx40231)
- The following message displays when a multilink PPP (MLP) bundle is configured with more than eight links:

  ```
  %RP_MLP-4-NODISTMLP: Failure downloading MLP bundle multilink1"
  ```

  This problem is resolved in Release 12.1(11b)E4. (CSCdx04754)
- More than nine MLP links are not supported on the FlexWAN. This problem is resolved in Release 12.1(11b)E4. (CSCin10249)

Resolved FlexWAN Module Caveats in Release 12.1(11b)E3

None.

Resolved FlexWAN Module Caveats in Release 12.1(11b)E2

None.

Resolved FlexWAN Module Caveats in Release 12.1(11b)E1

EoMPLS on FlexWan does not work. This problem is resolved in Release 12.1(11b)E1.

Resolved FlexWAN Module Caveats in Release 12.1(11b)E

None.

OSM Caveats

- Open OSM Caveats in Release 12.1(11b)E14, page 280
- Resolved OSM Caveats in Release 12.1(11b)E12, page 280
- Resolved OSM Caveats in Release 12.1(11b)E11, page 280
- Resolved OSM Caveats in Release 12.1(11b)E4, page 280
- Resolved OSM Caveats in Release 12.1(11b)E3, page 281
- Resolved OSM Caveats in Release 12.1(11b)E2, page 281
- Resolved OSM Caveats in Release 12.1(11b)E1, page 281
- Resolved OSM Caveats in Release 12.1(11b)E, page 281

Open OSM Caveats in Release 12.1(11b)E14

- PFC2-based QoS is supported on all the OSMs but has not been fully tested on the 2-port OC-12 ATM OSMs and the channelized OSMs. The PFC2 QoS CLI is not blocked for these modules, but we do not recommend that you configure PFC2-based QoS until testing has been completed. This problem is resolved in Release 12.1(12c)E1. (CSCdw84716)
- IGMP snooping does not function over an EoMPLS connection if the connection is made over a POS interface. There is no workaround. This problem is resolved in Release 12.1(13)E1. (CSCdw73064)
- Transmission of IP packets between MPLS clouds over (Generic Routing Encapsulation) GRE tunnels is not supported. This problem is resolved in Release 12.1(12c)E1. (CSCdw62753)
- In a configuration were global virtual routing and forwarding instance (VRF) routes are configured on a 4-port Gigabit Ethernet WAN OSM, when you ping a global IP address from a customer-edge device within a VPN, the ping fails. This failure occurs because a VRF-forwarding Gigabit Ethernet interface can resolve ARPs in the VRF ARP table, but it cannot be in the default ARP table. This problem is resolved in Release 12.1(12c)E1. (CSCdw74766, CSCin04666)
- If you use a subinterface on the 4-port Gigabit Ethernet WAN OSM to connect a Cisco 7600 series router or Catalyst 6500 series switch Provider Edge to an MPLS core, the VLAN ID on the subinterface must not coincide with the VLAN ID of the VLAN interface where the EoMPLS route is configured.

  Workaround: Assign a different VLAN ID for the subinterface. This problem is resolved in Release 12.1(13)E1. (CSCdv79130, CSCdw61392)

Resolved OSM Caveats in Release 12.1(11b)E14

None.

Resolved OSM Caveats in Release 12.1(11b)E12

None.

Resolved OSM Caveats in Release 12.1(11b)E11

None.

Resolved OSM Caveats in Release 12.1(11b)E4

- If you unconfigure routers using an MPLS VPN test script, occasionally the interface on the provider edge (PE) router is not to recognized after the virtual routing and forwarding instance (VRF) is deleted. This problem is resolved in Release 12.1(11b)E4. (CSCdx10237)
- Connected VPN routes may be missing from the MPLS forwarding table. This problem is resolved in Release 12.1(11b)E4. (CSCdx20720)
- Changes to the tagging status on links between provider to provider edge (PE) are not supported if more than one MPLS uplink is configured and the uplinks are loadsharing. This problem is resolved in Release 12.1(11b)E4. (CSCdx06042)
- In a topology where multiple MPLS uplinks have the same path cost, disabling MPLS IP on one of the uplinks may cause packet loss. This problem is resolved in Release 12.1(11b)E4. (CSCdx53564)
- After stress testing, an OIR of the OSM-OC12 POS module causes POS interfaces to repeatedly become active and inactive. This problem is resolved in Release 12.1(11b)E4. (CSCdx55544)

Resolved OSM Caveats in Release 12.1(11b)E3

None.

Resolved OSM Caveats in Release 12.1(11b)E2

Note All images in Release 12.1(11b)E2 are deferred.

The **set ip prec** and **set mpls exp** commands are not supported on main interfaces configured as VRF on the 4-port Gigabit Ethernet WAN OSM. This problem is resolved in Release 12.1(11b)E2. (CSCdx11904)

Resolved OSM Caveats in Release 12.1(11b)E1

None.

Resolved OSM Caveats in Release 12.1(11b)E

- Online Insertion and Removal (OIR) of any module in a chassis with OSMs and heavy traffic might occasionally cause an OSM to display the following message:

  ```
  FATAL ERROR:Fatal Management interrupt, gen_mgmt_intr_status 0x20,
  line_mgmt_intr_status 0x0, reloading
  ```

  This message indicates that the Parallel eXpress Forwarding (PXF) subsystem encountered a fatal error and caused the OSM to reload. There is no workaround. This problem is resolved in Release 12.1(11b)E. (CSCdu88920)

Release 12.1(8b)E and Rebuilds

- General Caveats, page 281
- FlexWAN Module Caveats, page 298
- OSM Caveats, page 301

General Caveats

- Open Caveats in Release 12.1(8b)E20, page 282
- Resolved Caveats in Release 12.1(8b)E20, page 283
- Resolved Caveats in Release 12.1(8b)E19, page 283
- Resolved Caveats in Release 12.1(8b)E18, page 284
- Resolved Caveats in Release 12.1(8b)E16, page 285
- Resolved Caveats in Release 12.1(8b)E15, page 285
- Resolved Caveats in Release 12.1(8b)E14, page 285
- Resolved Caveats in Release 12.1(8b)E13, page 288
- Resolved Caveats in Release 12.1(8b)E12, page 289
- Resolved Caveats in Release 12.1(8b)E11, page 290

- Resolved Caveats in Release 12.1(8b)E10, page 291
- Resolved Caveats in Release 12.1(8b)E9, page 292
- Resolved Caveats in Release 12.1(8b)E8, page 292
- Resolved Caveats in Release 12.1(8b)E7, page 293
- Resolved Caveats in Release 12.1(8b)E6, page 293
- Resolved Caveats in Release 12.1(8a)E5, page 295
- Resolved Caveats in Release 12.1(8a)E4, page 296
- Resolved Caveats in Release 12.1(8a)E3, page 297
- Resolved Caveats in Release 12.1(8a)E2, page 297
- Resolved Caveats in Release 12.1(8a)E, page 297

Open Caveats in Release 12.1(8b)E20

- Layer 3 hardware-switching support is not available for multicast traffic that needs to be fragmented and that passes through ingress and egress interfaces which have different MTU sizes. This problem is resolved in Release 12.1(13)E. (CSCdx95080)
- When you insert an SFM and transition the switching mode to truncated mode, QoS policing and marking stop working.

  Workaround: Remove and then reapply failed policy maps. (CSCeb20536)

  Note CSCeb20536 is not observed with later releases.

- If you delete a large number of routes (for example, 150,000), and then add new routes (for example, 800), traffic is not switched to the new routes.

  Workaround: Enter the **clear ip route *** command. This problem is resolved in Release 12.1(11b)E. (CSCdv58619, CSCeb16290)

- On a Layer 3 EtherChannel, applying an ACL to both the port-channel interface and a member port prevents the ACL from denying traffic correctly.

  Workaround: Remove the ACL from both the port-channel interface and the member port and reapply it only to the port-channel interface. This problem is resolved in Release 12.1(13)E5. (CSCdz56987)

- With a PFC2 and DFCs, do not configure SPAN sessions that include interfaces on fabric-enabled switching modules. This problem is resolved in Release 12.1(11b)E. (CSCds02430)
- If both IOS Server Load Balancing (SLB) and IOS Firewall Load Balancing (FWLB) are configured on the same router, ICMP packets that need to be firewall load balanced are routed by SLB instead. This problem is resolved in Release 12.1(12c)E2. (CSCdy18588)
- If you configure more than 16 HSRP group numbers for different VLAN interfaces in a system with a PFC1, the following error message is displayed:

  ```
  More than 16 standby groups not supported in this platform.
  ```

  This problem is resolved in Release 12.1(12c)E1. (CSCdx32496)

- In a system with a Supervisor Engine 1 and an MSFC1, individual Layer 2 aging commands for each VLAN might be present in the configuration file although only global Layer 2 aging has been configured. This problem is resolved in Release 12.1(11b)E. (CSCdv21083)

- After a system reset, the Layer 2 global aging timer value is reset to the default value of 300 seconds even though the startup configuration has the correct values.

  Workaround: Reconfigure the Layer 2 aging timer after a reset. This problem is resolved in Release 12.1(11b)E. (CSCdv21825)

- Jumbo frame support is incompatible with the IS-IS routing protocol. Leave the MTU size at the default value on any interface where IS-IS provides routing. This problem is resolved in Release 12.1(11b)E. (CSCdu09773, CSCdu48660)

- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) time stamp for the flash devices on a redundant supervisor engine. If you use applications that depend on ciscoFlashDeviceInitTime, take care not to remove a redundant supervisor engine or a Flash PC card from slave-slot0 when the applications are performing flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)

- Gigabit Ethernet ports might drop packets. The **show interfaces** command shows the dropped packets by displaying an incrementing overrun count. (CSCdy46165)

  Note CSCdy46165 is not observed with later releases.

Resolved Caveats in Release 12.1(8b)E20

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

  This problem is resolved in Release 12.1(8b)E20. (CSCei61732)

- Receipt of a Border Gateway Protocol (BGP) Autonomous System (AS) path with a length that is equal to or greater than 255 might reset the BGP session. This problem is resolved in Release 12.1(8b)E20. (CSCeh13489)

Resolved Caveats in Release 12.1(8b)E19

- When fragmenting MPLS traffic, a reload might occur after display of a “SYS-2-GETBUF” message. This problem is resolved in Release 12.1(8b)E19. (CSCeb16876)

- Receiving CDP packets with a host name that is 256 or more characters long might cause a memory leak in the CDP process. This problem is resolved in Release 12.1(8b)E19. (CSCin67568)

- With certain configurations, a reload might occur when you enter the **show cdp entry * protocol** command. This problem is resolved in Release 12.1(8b)E19. (CSCed40563)

- Many memory allocation failure (MALLOCFAIL) messages might occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
  Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  This problem is resolved in Release 12.1(8b)E19. (CSCdz32659)

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in Release 12.1(8b)E19. (CSCed93836, CSCdz84583)

Resolved Caveats in Release 12.1(8b)E18

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  This problem is resolved in Release 12.1(8b)E18. (CSCed27956, CSCed38527)

- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The

vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

This problem is resolved in Release 12.1(8b)E18. (CSCed28873)

Resolved Caveats in Release 12.1(8b)E16

- Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities. Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS). There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

  This problem is resolved in Release 12.1(8b)E16. (CSCea46342, CSCdx76632, CSCin56408, CSCdx40184, CSCec76776)
- The drop counters on Gigabit Ethernet interfaces might incorrectly increment excessively, even during low traffic conditions. No data is actually dropped. This problem is resolved in Release 12.1(8b)E16. (CSCdv86024)
- Incorrect VTP pruning might occur if you delete or rename VLANs in VLAN database mode. This problem is resolved in Release 12.1(8b)E16. (CSCeb60262)

Resolved Caveats in Release 12.1(8b)E15

- There might be OSPF neighbor drops and HSRP flaps when QoS is enabled on a Supervisor Engine 1 and MSFC2. This problem is resolved in Release 12.1(8b)E15. (CSCeb55271)

Resolved Caveats in Release 12.1(8b)E14

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.1(8b)E14. (CSCdu53656)
- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

This problem is resolved in Release 12.1(8b)E14. (CSCea28131)

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

  This problem is resolved in Release 12.1(8b)E14. (CSCdz71127, CSCea02355)

- With a Supervisor Engine 2 and a multicast receiver attached through a Layer 3 port on a WS-X6816-GBIC module and another receiver for the same multicast groups attached through a Layer 2 switchport, after a reset of the x6816 module, the Layer 3 port does not forward multicast traffic; or occasionally any forwarded multicast traffic is switched in software. This problem is resolved in Release 12.1(8b)E14. (CSCdy60173)
- When some multicast RPF interfaces are tunnel interfaces, a Supervisor Engine 1 with an MSFC1 might reload when the routing table changes frequently. This problem is resolved in Release 12.1(8b)E14. (CSCea50623)
- If MMLS is not synchronized between the MSFC and the supervisor engine when you enter a **clear ip mr *** command or a **clear ip mroute** *group_address* command, the MMLS entry on the supervisor engine might not be cleared. This problem is resolved in Release 12.1(8b)E14. (CSCdy51453)
- IEEE 802.1Q tunnel ports on WS-X6548-RJ45 switching modules drop ingress packets that are less than 68 bytes long when the packets are from a third-party device. This problem is resolved in Release 12.1(8b)E14. (CSCea50981)
- If a (S,G) state is created by receiving a prune at the source's first hop router, and then if the source starts sending, the registering process does not occur, which leads to the loss of multicast traffic. This usually happens when the source was sending traffic initially, and then stopped sending, and then starts sending again. This problem is resolved in Release 12.1(8b)E14. (CSCdw71336)
- If the NAT configuration on a flow's input and output interfaces indicate that NAT translation is required, the flow is switched in software even if no address translation mapping exists for the source. This problem is resolved in Release 12.1(8b)E14. (CSCdz33185)
- In an intermediate router where (*,G) and (S,G) traffic is RPF multicast fast dropped and the (*,G) traffic and the (S,G) traffic have different RPF interfaces, when an RPF change happens for the (S,G) entries, the intermediate router deletes the (S,G) entry but does not delete the (*,G) entry, which causes the multicast traffic to use (*,G) entry in HW and get dropped as non-RPF traffic. This problem is resolved in Release 12.1(8b)E14. (CSCea60918)
- In a redundant configuration that includes Supervisor Engine 2 running a Release 12.1(8a)E through Release 12.1(8b)E13 image, an SFM, and a WS-X6816-GBIC switching module, after a switch over to the redundant Supervisor Engine 2 due to a failure of the active Supervisor Engine 2, the previously active Supervisor Engine 2 keeps resetting and does not come up as the new redundant supervisor engine. This problem is resolved in Release 12.1(8b)E14. (CSCea43370)
- With a PFC2 and DFCs, do not configure SPAN sessions that include interfaces on fabric-enabled switching modules. This problem is resolved in Release 12.1(8b)E14. (CSCea07663)
- A reload might occur when you enter the **show scp mcast group 127** command or the command might wrongly display some processors to be part of group 127 that are not. This problem is resolved in Release 12.1(8b)E14. (CSCdz85864)

- Changes in the Unicast routing table can cause an inconsistency between software and hardware programming of the RPF interfaces of specific multicast groups. This inconsistency causes group-specific multicast traffic to be lost. This problem is resolved in Release 12.1(8b)E14. (CSCdz44110)
- With PIM configured and an (S,G) entry with the F flag reset, a directly connected source might not start registering when the source becomes active, and the (S,G) state might time out. This problem is resolved in Release 12.1(8b)E14. (CSCdz16276)
- With multicast support configured, a reload might occur when an interface flaps. This problem is resolved in Release 12.1(8b)E14. (CSCdy89663)
- When hardware switching is enabled, packets for (S,G) PR bit entry are not installed in hardware and are not forwarded using the (*,G) entry. This problem is resolved in Release 12.1(8b)E14. (CSCdy73313)
- To avoid a reload, do not enter the **clear ip igmp group** command while another user is displaying the output from the **show ip igmp group detail** command. This problem is resolved in Release 12.1(8b)E14. (CSCdy72767)
- To avoid a reload when PIM auto-rendezvous point (AutoRP) or bootstrap router (BSR) is configured, do not enter the **show ip pim rp mapping** command. This problem is resolved in Release 12.1(8b)E14. (CSCdy60995)
- In rare situations, an MSFC2 might freeze when it can receive control traffic from the supervisor engine, but it cannot send it. This problem is resolved in Release 12.1(8b)E14. (CSCdy15598)
- A reload might occur when you enter the **no ip routing** command. This problem is resolved in Release 12.1(8b)E14. (CSCdy02831)
- A reload might occur when you enter the **show ip mroute** command. This problem is resolved in Release 12.1(8b)E14. (CSCdx79227)
- A multilink PPP bundle might forward traffic intermittently. This problem is resolved in Release 12.1(8b)E14. (CSCdx48611)
- To avoid a reload, do not shut down any interfaces while another user is displaying the output from the **show ip pim neighbor** command. This problem is resolved in Release 12.1(8b)E14. (CSCdx25551)
- A reload might occur following a "%ALIGN-1-FATAL" message. This problem is resolved in Release 12.1(8b)E14. (CSCdx22902)
- A Gigabit Ethernet EtherChannel formed with DFC-supported ports and nonDFC-supported ports and configured not to use PAgP may stop passing traffic if you reset or OIR one of the Gigabit Ethernet switching modules. This problem is resolved in Release 12.1(8b)E14. (CSCdx00390)
- When an (S,G) entry with the T flag set transitions to an (S,G,R) entry an (S,G) RP-bit prune is sent towards the source instead of towards the RP. This problem is resolved in Release 12.1(8b)E14. (CSCdw95442)
- A multicast output interface might be added to the output interface list more than once. This problem is resolved in Release 12.1(8b)E14. (CSCdw54615)
- Following a **reload** command, the redundant supervisor engine might not boot properly. This problem is resolved in Release 12.1(8b)E14. (CSCdw39543)
- A reload might occur when you enter the **show ip mroute** command. This problem is resolved in Release 12.1(8b)E14. (CSCdw20251)

- If an output route-map in an EBGP neighbor has **match ip next-hop** or **match ip route-source** or **match ip community** or **match ip extcommunity** commands, then BGP updates might be incorrectly suppressed if the next-hop of the best path changes. This problem is resolved in Release 12.1(8b)E14. (CSCdv36378)
- With a network topology that creates an assert, after the assert winner prunes it's outgoing interface (which is correct), some neighbor routers might fail to override the prune with a join, which might break dense mode auto RP groups.This problem is resolved in Release 12.1(8b)E14. (CSCdv23921)
- The SNMP agent might send out trap using an incorrect IP address. This problem is resolved in Release 12.1(8b)E14. (CSCdv19638)
- On ingress interfaces, a (S,G) assert is not given priority over a (*,G) assert. This problem is resolved in Release 12.1(8b)E14. (CSCdv07210)
- Layer 3 multicast switching in hardware does not support multicast traffic through interfaces configured with secondary ip subnets. This problem is resolved in Release 12.1(8b)E14. (CSCdu71914)
- The **mls ip multicast stub command** does not support secondary ip subnets. This problem is resolved in Release 12.1(8b)E14. (CSCdu69367)
- The **distribute-list** *list_number* **out** *protocol protocol_number* command does not work. This problem is resolved in Release 12.1(8b)E14. (CSCdu52717)
- The **show ip route** command displays the Ethernet out-of-band (EOBC) interface, which should be hidden. This problem is resolved in Release 12.1(8b)E14. (CSCdw39211)
- The EOBC directly connected route (127.0.0.0/8) is entered into the routing protocol database and redistributed only if you enter the **redistribute connected** command for the protocol. This problem is resolved in Release 12.1(8a)E14. (CSCdt89766)
- The Open Shortest Path First (OSPF) designated router might generate router link states but not network link states for a connected network. The OSPF neighbors might come up correctly on all the routers in the network. This problem is resolved in Release 12.1(8b)E14. (CSCdu08686)
- PIM sparse mode for the Auto RP groups might not set the L flag for the RP discovery group. This problem is resolved in Release 12.1(8b)E14. (CSCdr51872, CSCdw13674)
- On a WS-X6816-GBIC switching module, the forwarding state of a VLAN on a trunk port or access port might be blocking when it should be forwarding. This problem is resolved in Release 12.1(8b)E14. (CSCdt93443)

Resolved Caveats in Release 12.1(8b)E13

- Cisco devices that run IOS and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default. The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at this URL:

  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

  This problem is resolved in Release 12.1(8b)E13. (CSCdz60229)

- Certain Cisco products containing support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default.

  Cisco will be making free software available to correct the problem as soon as possible.

  The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

  This problem is resolved in Release 12.1(8b)E13. (CSCdu75477)

- A Cisco Router that has run out of processor memory may unexpectedly reload due to a bus error at an invalid address if there is an attempt to connect with secure shell (ssh) into a vty port, which fails due to a process creation failure. A SYS-2-CFORKMEM error message appears before the restart. This problem is resolved in Release 12.1(8b)E13. (CSCdt13023)

Resolved Caveats in Release 12.1(8b)E12

- With a Supervisor Engine 1, traffic that fails the RPF test is not dropped in hardware. This problem is resolved in Release 12.1(8b)E12. (CSCdx94856)
- A reload might occur while displaying the group-rp mapping cache. This problem is resolved in Release 12.1(8b)E12. (CSCdw16433)
- The MSFC might run out of memory because of a memory leak in the routing table structures. This problem is resolved in Release 12.1(8b)E12. (CSCdy18789)
- When IGMP snooping is enabled on a switch that is between a multicast source and a multicast receiver, the switch incorrectly sends out two mtrace requests for each non-DVMRP-encapsulated mtrace request it receives. This problem is resolved in Release 12.1(8b)E12. (CSCdy47269)
- The IGMP Robustness Variable (defined in RFC 2236) is increased from 1 to 2 in Release 12.1(8b)E12. (CSCdt45806)
- With Supervisor Engine 2, packet loss might occur for a few seconds after routing protocol multicast packets are received. This problem is resolved in Release 12.1(8b)E12. (CSCdy58383)
- With Supervisor Engine 2, any access to an invalid address in the valid I/O address space can suspend all operation. This problem is resolved in Release 12.1(8b)E12. (CSCdx81901)
- If you configure an active member port of an EtherChannel as a SPAN source port, the port goes into the suspended state and does not pass any traffic. In Release 12.1(8b)E12, you cannot configure an active member port of an EtherChannel as a SPAN source port. (CSCdx81246)
- If you configure an EtherChannel between the Catalyst operating system and IOS on the supervisor engine and MSFC, the last port on the IOS device might not completely join the EtherChannel, which prevents multicast traffic from using the last port. This problem is resolved in Release 12.1(8b)E12. (CSCdy63364)
- With Supervisor Engine 2, multicast packets that set the router alert option, such as IGMP general queries and membership reports, might not be handled properly, which might disrupt IGMP client connectivity. This problem is resolved in Release 12.1(8b)E12. (CSCdy84078)
- Some malformed IGMP packets can loop through the system causing high CPU utilization. This problem is resolved in Release 12.1(8b)E12. (CSCdw41220)

- A failure in communication between the MSFC and the supervisor engine causes the MSFC to be reset by an internal message from the supervisor engine. This problem is resolved in Release 12.1(8b)E12. (CSCdx38960)
- Nonmaskable interrupts (NMIs) might cause a Supervisor Engine 1 to reload, and then the reload might fail. This problem is resolved in Release 12.1(8b)E12. (CSCdy25902)
- MAC address notifications to Layer 3 EtherChannels can be sent to the wrong ingress switching module. This problem is resolved in Release 12.1(8b)E12. (CSCdy47285)
- With a Supervisor Engine 2, (*,G) multicast entries are not programmed in hardware. This problem is resolved in Release 12.1(8b)E12. (CSCdy44937)
- If the shared tree and the shortest path tree (SPT) diverge because of a Reverse Path Forwarding (RPF) change on the shared tree (normally triggered by a restoration of a failed link), the SPT is pruned. A join to restore the traffic flow immediately follows the prune, which might interrupt traffic briefly. This problem is resolved in Release 12.1(8b)E12. (CSCdu74664)

Resolved Caveats in Release 12.1(8b)E11

- A malfunctioning DC-to-DC convertor on the WS-X6816 module affects the EOBC channel and causes the active supervisor engine to lose communication with other modules in the system.

  Workaround: Disable the power to the failed a WS-X6816 module from the CLI, or remove it from the system. This problem is resolved in Release 12.1(8b)E11. (CSCdx34821)
- NAT pool subranges are not working. This problem is resolved in Release 12.1(8b)E11. (CSCdt21533)
- Entering the **no interface portchannel** command, while running IP multicast traffic over a port channel interface causes a system reload. This problem is resolved in Release 12.1(8b)E11. (CSCdw93446)
- A sequencing problem results when there are NAT ACL configurations and static NAT entries in the startup configuration at bootup. The problem results in incorrect entries being programmed into the ternary content addressable memory (TCAM).

  Workaround: After bootup, remove the NAT configuration and reapply it. This problem is resolved in Release 12.1(8b)E11. (CSCdx35689)
- Entering the **show mls qos** [**ip** | **ipx** | **mac**] command in a system with a Supervisor Engine 1 causes a buffer of 64K to be allocated and never freed. This problem is resolved in Release 12.1(8b)E11. (CSCdx60833)
- VLANs in the 1002 to 1005 range are disabled by default in Catalyst software. In the Cisco IOS images for the Catalyst 6500 series and Cisco 7600 series router, the VLANs are in the forwarding state by default. This default discrepancy might cause a problem in a situation where a system running Release 12.1(8a)E3 or later on the supervisor engine and the MSFC is connected through an 802.1 Q tunnel to a system running Catalyst software. If the system running Cisco IOS software sends BPDUs for reserved VLANs in the 1002 to 1005 range, the system running Catalyst software drops these BPDUs and increments the rxTotalDrop counter.This problem is resolved in Release 12.1(8b)E11. (CSCdx28347)

Resolved Caveats in Release 12.1(8b)E10

- If you enter an invalid interface range for the SPAN sources or destinations, the SPAN feature may not work correctly and the system might reset. Changing the configuration to reflect a valid interface range corrects this problem. This problem is resolved in Release 12.1(8b)E10. (CSCdv07321, CSCdv07079)
- Setting the next hop for BGP route reflectors should be allowed only through the outbound route-map and not through the **nexthop-self** command. This problem is resolved in Release 12.1(8b)E10. (CSCdt84706)
- A packet encapsulation error occurs in DLSw. This problem is resolved in Release 12.1(8b)E10. (CSCdx20546)
- In a PFC2/MSFC2 system with a fabric-enabled 48-port 10/100 Mbps RJ45 module and a fabric-enabled 16 port 1000 Mbps GBIC module installed, when traffic enters the fabric-enabled 48-port 10/100 Mbps RJ45 and exits through the fabric-enabled 16 port 1000 Mbps GBIC module, or vice versa, dCEF forwarding is not enabled on the ingress module and traffic is dropped at the ingress port. This problem is resolved in Release 12.1(8b)E10. (CSCdw55635)
- Configuring protocol filtering on an interface to block IPX, AppleTalk, and other protocols also blocks egress IP and IPX traffic (ingress IP and IPX traffic is not affected). This problem is resolved in Release 12.1(8b)E10. (CSCdv23611)
- Enabling IGMP snooping causes multicast packets to be dropped. This problem is resolved in Release 12.1(8b)E10. (CSCdv24735)
- Partial component failures are not reported and do not trigger switchover in redundant supervisor engine configurations. This problem is resolved in Release 12.1(8b)E10. (CSCdw31630)
- If a system running Release 12.1(8b)E7 is used in a Server Load Balancing configuration, this error message may occur:

  ```
  Jan 13 19:17:08 MET: %ICC-5-WATERMARK: 1123 pkts for class L3-MGMT are waiting t o be
  processed
  ```

  This problem is resolved in Release 12.1(8b)E10. (CSCdw45465)
- The **mls aging fast** command has no effect. This problem is resolved in Release 12.1(8b)E10. (CSCdw66953)
- MAC address entries on DFCs do not age out. This problem is resolved in Release 12.1(8b)E10. (CSCdw76397)
- With IP or IPX ACLs configured on an interface, any incoming IPX packets with source and destination network numbers set to zero might get dropped on that interface. This problem is resolved in Release 12.1(8b)E10. (CSCdw76549)
- In a topology where two redundant routers are eligible to be distribution routers for a LAN, a PIM-SM router may see an interface in its Outgoing Interface List (OIL) with the expiration timer stuck and the outgoing interface never gets removed. This problem can occur when the backup distribution router is active, but the failed link from the primary distribution router is restored, causing the active distribution router status to change to from backup to primary.

  Workaround: Enter the **clear ip mroute** command. This problem is resolved in Release 12.1(8b)E10. (CSCdw80366)
- The supervisor engine reloads when a **write terminal** command is entered. This problem is resolved in Release 12.1(8b)E10. (CSCdw83512)

Resolved Caveats in Release 12.1(8b)E9

- An error can occur with management protocol processing. Use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  This problem is resolved in Release 12.1(8b)E9. (CSCdw65903)

Resolved Caveats in Release 12.1(8b)E8

- Enhanced IGRP (EIGRP) might display a "stuck in active" message with an incorrect network and mask (13.13.13.13 0xD0D0D0D). Routing is not affected. This problem is resolved in Release 12.1(8b)E8. (CSCdu78538)
- With the compress-config service enabled, if the configuration file is larger than the size of NVRAM, a "Not enough space on device" message is displayed when you enter the **copy rcp://***username@servername/config_name* **startup-config** command. This problem is resolved in Release 12.1(8b)E8. (CSCdu24409)
- Removing the last network statement for an area from an OSPF router configuration might cause a reload. This problem is resolved in Release 12.1(8b)E8. (CSCdw22714)
- The establishment of BGP peering might cause a spurious memory access or alignment error. Entering a clear bgp ip command might cause alignment errors. These errors typically have no operational impact, but with a very large number of neighbors, they might cause higher CPU usage. This problem is resolved in Release 12.1(8b)E8. (CSCdu02357)
- When a host that has been disconnected regains connectivity, an "Attempt to overwrite Sticky ARP entry" message might appear until the ARP table updates. This problem is resolved in Release 12.1(8b)E8. (CSCdu53957)
- The **ip cef load-sharing** command was not implemented. This problem is resolved in Release 12.1(8b)E8. (CSCdv12679)
- A Supervisor Engine 2 might display a draco2_inband_dma_pak message and reload. This problem is resolved in Release 12.1(8b)E8. (CSCdv88786)
- Configuring a reflexive ACL on a Supervisor Engine 1 with MSFC2 might cause a reload. This problem is resolved in Release 12.1(8b)E8. (CSCdw35672)
- The copy rcp://username@servername/config.name startup-config command fails if you specify a destination filename. This problem is resolved in Release 12.1(8b)E8. (CSCdw20118)
- With IGMP snooping enabled, configuring static routes might cause high CPU utilization and cause some multicast configurations to change from sparse mode to dense mode. This problem is resolved in Release 12.1(8b)E8. (CSCdw21276)
- NDE might display LINK-2-INTVULN traceback messages every 32 seconds. This problem is resolved in Release 12.1(8b)E8. (CSCdw29831)
- Reconfiguring ACLs might cause memory leaks. This problem is resolved in Release 12.1(8b)E8. (CSCdw14034)
- Files cannot be deleted from slot0. This problem is resolved in Release 12.1(8b)E8. (CSCdw37558)
- With Supervisor Engine 1 and MSFC or MSFC2, memory leaks occur with Releases 12.1(8b)E6 and 12.1(8b)E7. Entering the **show memory allocating-process totals | i L3** command will show that memory allocation to the Layer 3 manager has increased. This problem is resolved in Release 12.1(8b)E8. (CSCdw30661)

Resolved Caveats in Release 12.1(8b)E7

- For multicast flows, the PFC provides Layer 3 switching only when the ingress interface MTU size matches the minimum MTU size of the egress interface. This problem is resolved in Release 12.1(8b)E7. (CSCdu71710)
- Configuring broadcast suppression on a Gigabit Ethernet interface filters all broadcast traffic. This problem is resolved in Release 12.1(8b)E7. (CSCdv85377)
- When multiple switches configured with Supervisor Engine 1 and MSFC1 are connected to each other, in rare situations the MSFCs freeze temporarily while waiting for the neighboring MSFC to reply to an EIGRP query. The condition clears after MSFCs run through the default 3-minute SIA timer. This problem is resolved in Release 12.1(8b)E7. (CSCdv85419)
- The MSFC may reload after the **show ip igmp groups** command is entered if the command is paused for a prolonged period of time at the 'more' prompt and restarted later. This problem is resolved in Release 12.1(8b)E7. (CSCdu04678)
- If you change the configuration of a service policy, the **show policy-map interface** command displays incorrect statistics until you clear the policy map counters. This problem is resolved in Release 12.1(8b)E7. (CSCdr36213)
- With EIGRP, if a default network other than 0.0.0.0 and next hop are learned on an MSFC on a Supervisor Engine 1, and later the next hop changes, using either the same default network or a different default network, the MLS entries associated with the original next hop are not purged. This results in suboptimal routing or loss of traffic until you enter the **clear mls entry ip all** command to clear the MLS cache. This problem is resolved in Release 12.1(8b)E7. (CSCdt71961)
- An MSFC configured as a PIM router that receives a PIM sparse-mode JOIN/PRUNE message for the auto-RP groups causes those groups to transition from dense-mode forwarding to sparse-mode forwarding. This problem is resolved in Release 12.1(8b)E7. (CSCdu17859)
- The Open Shortest Path First (OSPF) database may not create the necessary entries to resubmit an OSPF interarea route. This problem is resolved in Release 12.1(8b)E7. (CSCdt93586)
- With data-link switching (DLSw) and Ethernet Redundancy (ER) configured, the MSFC might reload. This problem is resolved in Release 12.1(8b)E7. (CSCdv16277)
- With Enhanced Interior Gateway Routing Protocol (EIGRP) configured for any Layer 3 protocol (EIGRP-IP, EIGRP-IPX, and EIGRP-APPLETALK), the MSFC might reload. This problem is resolved in Release 12.1(8b)E7. (CSCdv04283)

Resolved Caveats in Release 12.1(8b)E6

- On a Supervisor Engine 1, during periods of very high route-update traffic, the pool of control message buffers might be exhausted. This problem is resolved in Release 12.1(8b)E6. (CSCdt73406)
- With a large number of multicast route entries with a large number of output interfaces (OIFs) for each entry, all multicast Layer 3 switching entries might get purged. This problem is resolved in Release 12.1(8b)E6. (CSCdv75054)
- With a redundant configuration, if a fan tray fails, the redundant supervisor engine does not become active if the active supervisor engine fails. This problem is resolved in Release 12.1(8b)E6. (CSCdv74489)
- NetFlow v7 records have an incorrect destination interface index if the MLS entry does not have an ingress SrcDstPorts entry. This problem is resolved in Release 12.1(8b)E6. (CSCdv11257)
- MBGP redistribution might not work as expected. Some autosummarization might take place instead. This problem is resolved in Release 12.1(8b)E6. (CSCdt62457)

- With Supervisor Engine 2, when a DVMRP unicast packet (for example, an MRINFO packet) enters the switch to be routed, the packet is replicated multiple times. The number of replications depends on the IP TTL value of the incoming packet. This problem is resolved in Release 12.1(8b)E6. (CSCdv62588)
- With Supervisor Engine 1, after entering the **no mls ip** and **mls ip** interface commands on an interface with multiple HSRP groups configured, some packets get switched in software on the MSFC. This problem is resolved in Release 12.1(8b)E6. (CSCdv62673)
- When configured to run OSPF, the MSFC might wrongly populate the OSPF router routing table with an entry corresponding to the MSFC itself, which can cause the MSFC to send a redundant Type-4 LSA. This problem is resolved in Release 12.1(8b)E6. (CSCdu40792)
- Redistributing OSPF default routes to RIP with a route map might produce incorrect results. This problem is resolved in Release 12.1(8b)E6. (CSCdu35038)
- An MSFC configured to support Data-Link Switching (DLSw) Ethernet redundancy might reload if the connection to an upstream device is lost. Examples of an upstream device include a router implementing SNA Switching Services (SNASw), a router with a connection to a mainframe through a Channel Interface Processor (CIP), or a Channel Port Adapter (CPA). This problem is resolved in Release 12.1(8b)E6. (CSCdu43189)
- ATM virtual circuits configured on an ATM port adapter in a FlexWAN module do not come up following an MSFC reload. This problem is resolved in Release 12.1(8b)E6. (CSCdu56182)
- When an MSFC is in the HSRP standby state, it incorrectly responds to the ARP_Request sent from an HSRP router in the Active state to a remote network beyond the MSFC in the HSRP standby state. This problem is resolved in Release 12.1(8b)E6. (CSCdv24926)
- CPU utilization increases incorrectly when any SLB virtual server or firewall farm is brought into service. This problem is resolved in Release 12.1(8b)E6. (CSCdv30472)
- When Internet Key Exchange (IKE) keepalive are not used, IPsec security associations are deleted when the IKE security association gets deleted. This is a change in Cisco IOS operation and causes backward compatibility issues with older versions, because IPsec security associations are up on the device using an older version. This problem is resolved in Release 12.1(8b)E6. (CSCdu37163)
- With MSFC2, when you enter the **ip forward-protocol turbo-flood** command and the **ip forward-protocol spanning-tree** command to forward UDP broadcasts on bridged interfaces, the forwarded packets on the lowest-numbered VLAN are corrupted. Other forwarded packets are not affected. This problem is resolved in Release 12.1(8b)E6. (CSCdv72780)
- A FlexWAN module might reload because of a spurious memory access at the hqf_cwpa_pak_enqueue_local process. This problem is resolved in Release 12.1(8b)E6. (CSCdu80042)
- Entering the **show ip cef exact-route** command at the transmit end of a MultiProtocol Label Switching (MPLS) Traffic Engineering (TE) tunnel might cause the MSFC2 to reload. This situation occurs when the destination prefix is recursive and the MSFC2 is load sharing to the next hop. This problem is resolved in Release 12.1(8b)E6. (CSCdt80914)
- An RPF check incorrectly prefers BGP over MBGP when both tables have the same match route and there is no BGP or MBGP distance configured. This problem is resolved in Release 12.1(8b)E6. (CSCdv47188)
- A BGP route reflector is not advertising a MBGP route correctly. This problem is resolved in Release 12.1(8b)E6. (CSCdv35791)
- The switch might reload if you use the range keyword to enter the **switchport** command. This problem is resolved in Release 12.1(8b)E6. (CSCdv17531)

- When data-link switching (DLSw) Ethernet redundancy is configured, the switch might reload with a bus error if circuits are established while peer connections are torn down. This problem is resolved in Release 12.1(8b)E6. (CSCdt82241)
- After entering **shutdown** and **no shutdown** commands on an interface running fast switching, some of the route cache entries for directly connected hosts are not created correctly, which causes network connectivity issues. This problem is resolved in Release 12.1(8b)E6. (CSCdv43186)
- Suboptimal routes might be installed into the routing table if more then the configured number of equal cost paths exist. This problem is resolved in Release 12.1(8b)E6. (CSCdu41228)

Resolved Caveats in Release 12.1(8a)E5

- It is possible to send an ARP packet to a local Ethernet device running on specific versions of Cisco IOS, which could cause that interface to stop sending and receiving traffic. ARP packets received by the router for the router's own interface address but a different MAC address will overwrite the router's MAC address in the ARP table with the one from the received ARP packet. This was demonstrated to attendees of the Black Hat conference and should be considered to be public knowledge. This attack is only successful against devices on the Ethernet segment local to the attacker or attacking host.

  This vulnerability is documented in Cisco Bug ID CSCdu81936, and a workaround is available.

  The workaround for this vulnerability is to enter the router interface MAC address into the ARP table with a configuration entry, sometimes known as “hard coding” the ARP table entry.

  The syntax for this command for routers and switches running IOS is as follows:

  arp *ip_address hardware_address type* [**alias**]

  The syntax for this command for switches running Catalyst software is as follows:

  set arp [**dynamic | permanent | static**] *ip_address hardware_address*

  The caveat to this workaround is identified with defect CSCdv04366, which will clear all manually entered MAC addresses from the ARP table, when they are the same as the interface MAC address, when the command **clear arp** is issued on the router.

  This problem is resolved in Release 12.1(8a)E5. (CSCdu81936)
- Some policy-based routing configurations that divert traffic to external devices for additional processing (for example, to a firewall) might incorrectly divert the traffic again after it has been processed by the external device. This problem is resolved in Release 12.1(8a)E5. (CSCds60420)
- An MSFC2 might reload if you remove a default static route that was recursively learned from multiple paths. This problem is resolved in Release 12.1(8a)E5. (CSCdv46440)
- In an Anycast multicasting environment, the convergence time is too long when the link to one rendezvous point (RP) goes down and the receiver’s designated router (DR) needs to send join messages to another RP. This problem is resolved in Release 12.1(8a)E5. (CSCdv27799)
- When redistributing RIPv2 tagged routes to another routing protocol, route filtering fails in route maps configured with the **match tag** command. This problem is resolved in Release 12.1(8a)E5. (CSCdt71063)
- When heavy traffic causes significant TCP latency, closing an established connection might cause memory leakage of the TCB, which you can display by entering the **show tcp brief** or **show tcp brief all** command. The leaked TCB will be in the TIMEWAIT state. This problem is resolved in Release 12.1(8a)E5. (CSCdu79634)

- Adding or removing an entry from the IGMP cache for special addresses 224.0.1.39 or 224.0.1.40 or 224.0.0.x or an interface joining or leaving a multicast group unnecessarily resets the interface hardware, causing the interface to go down and then back up. This problem is resolved in Release 12.1(8a)E5. (CSCdv43208)
- Entering the **attach** command while connected over a secure shell (SSH) session freezes the switch. This problem is resolved in Release 12.1(8a)E5. (CSCdm78585)
- With AAA accounting enabled, TFTP downloads take much longer. This problem is resolved in Release 12.1(8a)E5. (CSCdt42050)
- EIGRP routing updates about routes configured with the **redistribute connected** command are not processed correctly. This problem is resolved in Release 12.1(8a)E5. (CSCdu59583)
- When the Cisco IOS server load balancing stateful backup feature sends updates for connections that have been both server load balanced and firewall load balanced, the firewall real information is not transported in the connection update. This problem is resolved in Release 12.1(8a)E5. (CSCdv22951)
- The **snmp trap link-status** command is not saved when you enter the **write memory** and **reload** commands. After you enter the **snmp trap link-status** command, the **no snmp trap link-status** command has no effect. This problem is resolved in Release 12.1(8a)E5. (CSCdv03931)
- When a Layer 3 interface goes down, there is up to a 1-second delay before the MSFC is notified, which results in a convergence time of approximately 2 seconds in the Layer 3 redundant environment. This problem is resolved in Release 12.1(8a)E5. (CSCdt44165)
- After multiple online insertion and removal (OIR) operations on an OC12 or OC48 optical services module (OSM), the running configuration for the slot may be lost and the OIR may fail. This problem is resolved in Release 12.1(8a)E5. (CSCdv11985)
- The switch might reload due to a bus error in process_events_waiting_p. This problem is resolved in Release 12.1(8a)E5. (CSCdv46280)

Resolved Caveats in Release 12.1(8a)E4

- A Telnet connection through an OC-12/vip4-80 either times out or is too slow to process commands. This problem also affects other applications such as FTP and HTTP. This problem is resolved in Release 12.1(8a)E4. (SCSdv09097)
- With Release 12.1(8a)E and later releases, when you configure the spanning tree port-priority on an access port, a line entry is created for all the VLANs even if they are not in the VLAN database. This problem is resolved in Release 12.1(8a)E4. (CSDdv03102)
- A race condition exists when hidden VLAN updates and trunking information is processed by the OSM-4GE-WAN modules. If the trunking information is processed first, the main interface fails to ping. This problem is resolved in Release 12.1(8a)E4. (CSCdv21981)
- When the NAT outside-source static translation is configured, packets are forwarded without translation. This problem is resolved in Release 12.1(8a)E4. (CSCdv12429)
- Configuring IPX NLSP causes a system reset. This problem is resolved in Release 12.1(8a)E4. (CSCdu63323)
- Partially switched multicast packets coming from an OSM interface might trigger an MSFC reset. This problem is resolved in Release 12.1(8a)E4. (CSCdv24728)
- If a switch is responding to hosts using proxy ARP and has multiple paths to a destination network, the switch might forward packets for the host for which it is performing the proxy ARP to the interface the switch proxied to if the primary path fails or a new path with a lower metric is added. This problem is resolved in Release 12.1(8a)E4. (CSCdu47015)

Resolved Caveats in Release 12.1(8a)E3

None.

Resolved Caveats in Release 12.1(8a)E2

- In systems with a Supervisor Engine 1, entering the **show mls nde** command shows the NetFlow Data Export feature as disabled when it is enabled. This problem occurs if you enter an **ip flow-export** command after the **mls nde src_address** command and do not reenter the **mls nde src_address** command. This problem is resolved in Release 12.1(8a)E2 with the introduction of the new [**no**] **mls nde sender** [**version** *version*] command, which replaces the [**no**] **mls nde src_address** *ip_address* [**version** *version*] command.

  When an image with the new **mls nde sender** command is run on a system containing the old command **mls nde src_address**, the old command is still accepted, but he source address specified by this command is not used. Instead, the new image takes the NDE source from the **ip flow export source** *interface* command configuration. When you enter the **write memory** command, the new image replaces the old **mls nde src_address** *ip_address* [**version** *version*] in the configuration with the new **mls nde sender** [**version** *version*] command. The **mls nde sender** command supports NDE version 7 only. This problem is resolved in Release 12.1(8a)E2. (CSCdu56084)
- When you configure VINES routing, all MSFC2s autoconfigure the same VINES node number. This problem is resolved in Release 12.1(8a)E2. (CSCdu03802)
- IGMP snooping suppresses IGMP membership reports incorrectly if a response to a group-specific query is received during the query-max-response-time of a general query but after a membership report has been received. As a result, the response to the group-specific query may not be forwarded to the router. This problem might cause a multicast stream to be interrupted until the next general query is sent. This problem is resolved in Release 12.1(8a)E2. (CSCdu62075)

Resolved Caveats in Release 12.1(8a)E

- With a PFC2, you cannot attach QoS policies to VLANs; do not enter the **mls qos vlan-based** command. This problem is resolved in Release 12.1(8a)E. (CSCdu36187)
- Encrypted VPN traffic might cause a reload. This problem is resolved in Release 12.1(8a)E. (CSCdt63735, CSCdt79571)
- Configuring DLSW might cause memory corruption or reloads on an MSFC2. This problem is resolved in Release 12.1(8a)E. (CSCdu13015, CSCdu06210)
- The MSFC2 does not support the MultiNode Load Balancing (MNLB) forwarding agent of the MNLB feature set for LocalDirector. This problem is resolved in Release 12.1(8a)E. (CSCdr65433)
- If a route map with only one clause is applied to an interface, and no other feature is applied to the interface, the TCAM might be programmed so that traffic that is supposed to be policy-routed on that interface is routed normally, and traffic that is supposed to be routed normally on that interface is dropped. This problem is resolved in Release 12.1(8a)E. (CSCdu50320)
- With Supervisor Engine 2, when you configure more than 25 input Cisco IOS ACLs, only the first 25 work; instead of permitting traffic, all other Cisco IOS ACLs incorrectly drop traffic. This problem is resolved in Release 12.1(8a)E. (CSCdu36594)
- The EtherChannel SNMP HC counters occasionally return a zero value and sometimes return values associated with only one of the physical ports for an SNMP query that occurs when the EtherChannel interface counters are being updated. This problem is resolved in Release 12.1(8a)E. (CSCdu44931)

- The **show version** command might display “Running default software” instead of the boot filename. This problem is resolved in Release 12.1(8a)E. (CSCdu23762)
- With Supervisor Engine 2, ignore any “%BIT-SP-4-OUTOFRANGE: bit 16 is not in the expected range of 0 to -1” error messages. This problem is resolved in Release 12.1(8a)E. (CSCdu26072)
- The **crypto map** interface command is disabled to prevent a reload. This problem is resolved in Release 12.1(8a)E. (CSCdt56832)
- With very heavy traffic, online insertion or removal of a WS-X6408-GBIC or WS-X6408A-GBIC 8-port Gigabit Ethernet switching module might cause the supervisor engine to reload. This problem is resolved in Release 12.1(8a)E. (CSCdt91705)
- You might see “c6k_stack_mib_module_added:error 3 from idprom_image_find()” error messages during boot up. This problem is resolved in Release 12.1(8a)E. (CSCdt87637)
- You cannot configure the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr62024, CSCdr54103)
- No warning message displays if you exceed the maximum number (63) of microflow policers. The extra policers are displayed by the **show mls qos ip** command, but they do not work. If classes are increased beyond the maximum number (255) in a policy-map, the policy is rejected without a warning message if applied to an interface. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(6)E. (CSCds38349, CSCdt38130)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(8b)E20, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E20, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E19, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E18, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E17, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E16, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E15, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E14, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E13, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E12, page 299
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E11, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E10, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E9, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E8, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E7, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8b)E6, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8a)E5, page 300

- Resolved FlexWAN Module Caveats in Release 12.1(8a)E4, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8a)E3, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8a)E2, page 300
- Resolved FlexWAN Module Caveats in Release 12.1(8a)E, page 300

Open FlexWAN Module Caveats in Release 12.1(8b)E20

- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan***slot_number/port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module crashinfo file with the **copy cwan***slot_number/port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)

Resolved FlexWAN Module Caveats in Release 12.1(8b)E20

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E19

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E18

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E17

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E16

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E15

- With dial-up networking (DUN) configured, the IP Control Protocol (IPCP) times out on a link control protocol (LCP) negotiation. This problem is resolved in Release 12.1(8b)E15. (CSCea51540)

Resolved FlexWAN Module Caveats in Release 12.1(8b)E14

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E13

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E12

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E11

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E10

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E9

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E8

None.

Resolved FlexWAN Module Caveats in Release 12.1(8b)E7

- Entering **shutdown** and **no shutdown** commands for a FlexWAN module multilink interface might cause the FlexWAN module to reload. If the link connects two FlexWAN modules, both modules might reload. This problem is resolved in Release 12.1(8b)E7. (CSCdu75389)

Resolved FlexWAN Module Caveats in Release 12.1(8b)E6

None.

Resolved FlexWAN Module Caveats in Release 12.1(8a)E5

- With MLS IP multicast enabled, FlexWAN ATM interfaces drop multicast traffic destined for the MSFC. This problem is resolved in Release 12.1(8a)E5. (CSCdv33657)

Resolved FlexWAN Module Caveats in Release 12.1(8a)E4

- In a switch with FlexWAN modules, nonfabric-enabled modules, fabric-enabled modules, and an SFM, traffic on the FlexWAN module interfaces is discarded after an OIR of any nonfabric-enabled module. This problem is resolved in Release 12.1(8a)E4. (CSCdv10649)

Resolved FlexWAN Module Caveats in Release 12.1(8a)E3

- If Multicast MLS is enabled on the ingress Layer 3 interface, the FlexWAN module drops ATM VC egress multicast traffic. This problem is resolved in Release 12.1(8a)E3. (CSCdu83619)

Resolved FlexWAN Module Caveats in Release 12.1(8a)E2

None.

Resolved FlexWAN Module Caveats in Release 12.1(8a)E

- Flows between an Ethernet interface configured with an HSRP standby IP address and a WAN interface might not be Layer 3 switched. This problem is resolved in Release 12.1(8a)E. (CSCds66364)

OSM Caveats

- Open OSM Caveats in Release 12.1(8b)E20, page 301
- Resolved OSM Caveats in Release 12.1(8b)E20, page 301
- Resolved OSM Caveats in Release 12.1(8b)E19, page 301
- Resolved OSM Caveats in Release 12.1(8b)E18, page 301
- Resolved OSM Caveats in Release 12.1(8b)E17, page 302
- Resolved OSM Caveats in Release 12.1(8b)E16, page 302
- Resolved OSM Caveats in Release 12.1(8b)E15, page 302
- Resolved OSM Caveats in Release 12.1(8b)E14, page 302
- Resolved OSM Caveats in Release 12.1(8b)E13, page 302
- Resolved OSM Caveats in Release 12.1(8b)E12, page 302
- Resolved OSM Caveats in Release 12.1(8b)E11, page 302
- Resolved OSM Caveats in Release 12.1(8b)E10, page 302
- Resolved OSM Caveats in Release 12.1(8b)E9, page 302
- Resolved OSM Caveats in Release 12.1(8b)E8, page 302
- Resolved OSM Caveats in Release 12.1(8b)E7, page 302
- Resolved OSM Caveats in Release 12.1(8b)E6, page 302
- Resolved OSM Caveats in Release 12.1(8a)E5, page 303
- Resolved OSM Caveats in Release 12.1(8a)E4, page 303

Open OSM Caveats in Release 12.1(8b)E20

- Online Insertion and Removal (OIR) of any module in a chassis with OSMs and with heavy traffic might occasionally cause an OSM to display the following message:

  ```
  FATAL ERROR:Fatal Management interrupt, gen_mgmt_intr_status 0x20,
  line_mgmt_intr_status 0x0, reloading
  ```

  This message indicates that the Parallel eXpress Forwarding (PXF) subsystem encountered a fatal error and caused the OSM to reload. There is no workaround. This problem is resolved in Release 12.1(11b)E. (CSCdu88920)

Resolved OSM Caveats in Release 12.1(8b)E20

None.

Resolved OSM Caveats in Release 12.1(8b)E19

None.

Resolved OSM Caveats in Release 12.1(8b)E18

None.

Resolved OSM Caveats in Release 12.1(8b)E17

None.

Resolved OSM Caveats in Release 12.1(8b)E16

None.

Resolved OSM Caveats in Release 12.1(8b)E15

- For virtual private dial-up networks (VPDN), when an L2TP access concentrator (LAC) negotiates an authentication protocol that is not listed as a valid authentication protocol according to the L2TP Network Server (LNS) configuration, the LNS incorrectly accepts the negotiated options and uses the authentication protocol set by the LAC. This problem is resolved in Release 12.1(8b)E15. (CSCdz83019)

Resolved OSM Caveats in Release 12.1(8b)E14

None.

Resolved OSM Caveats in Release 12.1(8b)E13

None.

Resolved OSM Caveats in Release 12.1(8b)E12

None.

Resolved OSM Caveats in Release 12.1(8b)E11

None.

Resolved OSM Caveats in Release 12.1(8b)E10

None.

Resolved OSM Caveats in Release 12.1(8b)E9

None

Resolved OSM Caveats in Release 12.1(8b)E8

None.

Resolved OSM Caveats in Release 12.1(8b)E7

None.

Resolved OSM Caveats in Release 12.1(8b)E6

None.

Resolved OSM Caveats in Release 12.1(8a)E5

- When the fiber-optic cable carrying traffic from the add-drop multiplexer (ADM) is removed from a packet-over-SONET (POS) interface, the automatic protection switchover (APS) does not occur. This problem is resolved in Release 12.1(8a)E5. (CSCdv53401)
- If an Optical Services Modules (OSM) has three or more Gigabit Interface Converters (GBICs) with no link, CPU utilization on the OSM increases and some functions of the OSM, such as a module image upgrade by the MSFC2, take much longer than normal or fail to complete. This problem is resolved in Release 12.1(8a)E5. (CSCdu83474)

Resolved OSM Caveats in Release 12.1(8a)E4

- OSMs might go down after an MSFC reload. This problem is resolved in Release 12.1(8a)E4. (CSCdv24580, CSCdv12202)

Release 12.1(7a)E and Rebuilds

- General Caveats, page 303
- FlexWAN Module Caveats, page 304

General Caveats

- Open Caveats in Release 12.1(7a)E6, page 303
- Resolved Caveats in Release 12.1(7a)E6, page 304
- Resolved Caveats in Release 12.1(7a)E1, page 304
- Resolved Caveats in Release 12.1(7)E, page 304

Open Caveats in Release 12.1(7a)E6

- If both IOS Server Load Balancing (SLB) and IOS Firewall Load Balancing (FWLB) are configured on the same router, ICMP packets that need to be firewall load balanced are routed by SLB instead. This problem is resolved in Release 12.1(12c)E2. (CSCdy18588)
- The **crypto map** interface command is disabled to prevent a reload. This problem is resolved in Release 12.1(8a)E. (CSCdt56832)
- Jumbo frame support is incompatible with the IS-IS routing protocol. Leave the MTU size at the default value on any interface where IS-IS provides routing. This problem is resolved in Release 12.1(11b)E. (CSCdu09773)
- With very heavy traffic, online insertion or removal of a WS-X6408-GBIC or WS-X6408A-GBIC 8-port Gigabit Ethernet switching module might cause the supervisor engine to reload. This problem is resolved in Release 12.1(8a)E. (CSCdt91705)
- It is safe to ignore c6k_stack_mib_module_added:error 3 from idprom_image_find() error messages during boot up. This problem is resolved in Release 12.1(8a)E. (CSCdt87637)
- When you configure VINES routing, all MSFC2s autoconfigure the same vines node number. The workaround is to enter the **vines routing recompute** command. This problem is resolved in Release 12.1(8a)E2. (CSCdu03802)
- The MSFC2 does not support the MultiNode Load Balancing (MNLB) forwarding agent of the MNLB feature set for LocalDirector. This problem is resolved in Release 12.1(8a)E. (CSCdr65433)

- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) time stamp for the Flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor engine or a PCMCIA card from slave-slot0 when the applications are performing Flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)

Resolved Caveats in Release 12.1(7a)E6

- An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  This problem is resolved in Release 12.1(7a)E6. (CSCdw65903)

Resolved Caveats in Release 12.1(7a)E1

- After erasing the NVRAM and rebooting the system, the line protocol might not come up on some interfaces. This problem is resolved in Release 12.1(7a)E1. (CSCdu09356)

Resolved Caveats in Release 12.1(7)E

- The **crypto map** interface command causes a reload. This command is disabled in Release 12.1(7)E. (CSCdu03017)
- You cannot configure the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr62024, CSCdr54103)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(7a)E6, page 304
- Resolved FlexWAN Module Caveats in Release 12.1(7a)E6, page 305
- Resolved FlexWAN Module Caveats in Release 12.1(7a)E1, page 305
- Resolved FlexWAN Module Caveats in Release 12.1(7)E, page 305

Open FlexWAN Module Caveats in Release 12.1(7a)E6

- Flows between an Ethernet interface configured with an HSRP standby IP address and a WAN interface might not be Layer 3 switched. This problem is resolved in Release 12.1(8a)E. (CSCds66364)
- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan***slot_number/port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module **crashinfo** file with the **copy cwan***slot_number/port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)
- To use the interfaces on the FlexWAN module, you must enable IP routing on the MSFC. (CSCdp34896)

Resolved FlexWAN Module Caveats in Release 12.1(7a)E6

None.

Resolved FlexWAN Module Caveats in Release 12.1(7a)E1

None.

Resolved FlexWAN Module Caveats in Release 12.1(7)E

None.

Release 12.1(6)E and Rebuilds

- General Caveats, page 305
- FlexWAN Module Caveats, page 307

General Caveats

- Open Caveats in Release 12.1(6)E8, page 305
- Resolved Caveats in Release 12.1(6)E8, page 306
- Resolved Caveats in Release 12.1(6)E1, page 306
- Resolved Caveats in Release 12.1(6)E, page 306

Open Caveats in Release 12.1(6)E8

- Secure shell (SSH) support does not work with MSFC2. This problem is resolved in Release 12.1(8a)E. (CSCdt56832)
- If both IOS Server Load Balancing (SLB) and IOS Firewall Load Balancing (FWLB) are configured on the same router, ICMP packets that need to be firewall load balanced are routed by SLB instead. This problem is resolved in Release 12.1(12c)E2. (CSCdy18588)
- You cannot configure the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr62024, CSCdr54103)
- The MSFC2 does not support the MultiNode Load Balancing (MNLB) forwarding agent of the MNLB feature set for LocalDirector. This problem is resolved in Release 12.1(8a)E. (CSCdr65433)
- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) time stamp for the Flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor engine or a PCMCIA card from slave-slot0: when the applications are performing Flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)

Resolved Caveats in Release 12.1(6)E8

- An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  This problem is resolved in Release 12.1(6)E8. (CSCdw65903)

Resolved Caveats in Release 12.1(6)E1

- When the active supervisor engine shuts down normally, it notifies the redundant supervisor engine to switch over quicker. Occasionally, this notification fails, resulting in an infinite series of SYS-2-INTSCHED messages. This problem is resolved in Releases 12.1(5c)E10 and 12.1(6)E1. (CSCdt21103)
- Occasionally, the active supervisor engine fails to send clock updates to the redundant supervisor engine, which hangs the heartbeat process on the active supervisor engine. This causes the system to reload. This problem is resolved in Releases 12.1(5c)E10 and 12.1(6)E1. (CSCdt28184)
- With a large OSPF routing table, the MSFC might experience periods of high CPU utilization and temporary loss of console communication when redistributing routes. This problem is resolved in Releases 12.1(5c)E10 and 12.1(6)E1. (CSCdt71785)

Resolved Caveats in Release 12.1(6)E

- No warning message displays if you exceed the maximum number (63) of microflow policers. The extra policers are displayed by the **show mls qos ip** command, but they do not work. If classes are increased beyond the maximum number (255) in a policy map, the policy is rejected without a warning message if applied to an interface.For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(6)E. (CSCds38349, CSCdt38130)
- When IGMP snooping receives a GS query, it always replies with a join message. IGMP snooping should only reply to the GS query if there is at least one nonrouter host port other than the port from which it received the GS query. This problem is resolved in Release 12.1(6)E. (CSCdt51303)
- The **verify** command fails when used on a file in the sup-bootflash device. This problem is resolved in Release 12.1(6)E. (CSCdt09870)
- Occasionally, when IGMP snooping is enabled, some Layer 3-switched multicast groups might stop forwarding traffic. This problem is resolved in Release 12.1(6)E. (CSCds28792)
- When VTP traps are enabled and a VTP trap is generated because a version 1 VTP device is detected, communication between the supervisor engine and the MSFC might fail, which causes a reload. This problem is resolved in Release 12.1(6)E. (CSCdt44708)
- Downloading images to an Intel Value series 200 Flash card in the PCMCIA slot may in rare situations fail to write a valid image. This problem is resolved in Release 12.1(6)E (see the related Release 12.0(7)XE1 resolved CSCdm52806 caveat). (CSCdm52806)
- The **copy running-config startup-config** command does not save the **boot system flash** command in the startup configuration file. Enter the **write memory** command instead. This problem is resolved in Release 12.1(6)E. (CSCds43994)
- Changes to the **boot system flash** command in the startup configuration file are not always copied to the corresponding ROMMON variable. This problem is resolved in Release 12.1(6)E. (CSCdt06423)

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(6)E8, page 307
- Resolved FlexWAN Module Caveats in Release 12.1(6)E8, page 307
- Resolved FlexWAN Module Caveats in Release 12.1(6)E1, page 307
- Resolved FlexWAN Module Caveats in Release 12.1(6)E, page 307

Open FlexWAN Module Caveats in Release 12.1(6)E8

- Flows between an Ethernet interface configured with an HSRP standby IP address and a WAN interface might not be Layer 3 switched. This problem is resolved in Release 12.1(8a)E. (CSCds66364)
- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan***slot_number/port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module **crashinfo** file with the **copy cwan***slot_number/port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)
- To use the interfaces on the FlexWAN module, you must enable IP routing on the MSFC. (CSCdp34896)

Resolved FlexWAN Module Caveats in Release 12.1(6)E8

None.

Resolved FlexWAN Module Caveats in Release 12.1(6)E1

None.

Resolved FlexWAN Module Caveats in Release 12.1(6)E

- When converting from Catalyst software to Cisco IOS, the **show interfaces** command for the FlexWAN module might display “administratively down, line protocol is down.” This problem is resolved in Release 12.1(6)E. (CSCds86384)
- Flows for packets larger than 1500 bytes might not be Layer 3 switched. This problem is resolved in Release 12.1(6)E. (CSCds66329)

Release 12.1(5c)E and Rebuilds

- General Caveats, page 305
- FlexWAN Module Caveats, page 307

General Caveats

- Open Caveats in Release 12.1(5c)E12, page 308
- Resolved Caveats in Release 12.1(5c)E12, page 308
- Resolved Caveats in Release 12.1(5c)E10, page 309
- Resolved Caveats in Release 12.1(5c)E9, page 309

- Resolved Caveats in Release 12.1(5c)E8, page 309
- Resolved Caveats in Release 12.1(5a)E3, page 311
- Resolved Caveats in Release 12.1(5a)E1, page 311
- Resolved Caveats in Release 12.1(5a)E, page 312

Open Caveats in Release 12.1(5c)E12

- Secure shell (SSH) support does not work with MSFC2. This problem is resolved in Release 12.1(8a)E. (CSCdt56832)
- You cannot configure the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr62024, CSCdr54103)
- The **copy running-config startup-config** command does not save the **boot system flash** command in the startup configuration file. Enter the **write memory** command instead. This problem is resolved in Release 12.1(6)E. (CSCds43994)
- No warning message displays if you exceed the maximum number (63) of microflow policers. The extra policers are displayed by the **show mls qos ip** command, but they do not work. If classes are increased beyond the maximum number (255) in a policy-map, the policy is rejected without a warning message if applied to an interface. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(6)E. (CSCds38349)
- The MSFC2 does not support the MultiNode Load Balancing (MNLB) forwarding agent of the MNLB feature set for LocalDirector. This problem is resolved in Release 12.1(8a)E. (CSCdr65433)
- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) time stamp for the Flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor engine or a PCMCIA card from slave-slot0: when the applications are performing Flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- Downloading images to an Intel Value series 200 Flash card in the PCMCIA slot may in rare situations fail to write a valid image. Downloading during periods of low system activity reduces the likelihood of this failure. This problem is resolved in Release 12.1(6)E (see the related Release 12.0(7)XE1 resolved CSCdm52806 caveat). (CSCdm52806)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)

Resolved Caveats in Release 12.1(5c)E12

- An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  This problem is resolved in Release 12.1(5c)E12. (CSCdw65903)

Resolved Caveats in Release 12.1(5c)E10

- When the active supervisor engine shuts down normally, it notifies the redundant supervisor engine to switch over quicker. Occasionally, this notification fails, resulting in an infinite series of SYS-2-INTSCHED messages. This problem is resolved in Releases 12.1(5c)E10 and 12.1(6)E1. (CSCdt21103)
- Occasionally, the active supervisor engine fails to send clock updates to the redundant supervisor engine, which hangs the heartbeat process on the active supervisor engine. This causes the system to reload. This problem is resolved in Releases 12.1(5c)E10 and 12.1(6)E1. (CSCdt28184)
- With a large OSPF routing table, the MSFC might experience periods of high CPU utilization and temporary loss of console communication when redistributing routes. This problem is resolved in Releases 12.1(5c)E10 and 12.1(6)E1. (CSCdt71785)

Resolved Caveats in Release 12.1(5c)E9

- Maximum-sized packets sent to a tunnel interface on an MSFC2 cause a reload. To avoid the problem, tunnel traffic is process switched in Release 12.1(5c)E9 and later. (CSCdt04991)

Resolved Caveats in Release 12.1(5c)E8

- Cisco Security Advisory:
  Cisco IOS Software TCP Initial Sequence Number Randomization Improvements
  Revision 1.0: INTERIM
  For Public Release2001 February 27 20:00 US/Eastern (UTC+0500)

  Summary:

  Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

  This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

  To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

  Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices. This notice will be posted at:

  http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml. (CSCds04747)
- With an MSFC2, HSRP does not work on VLANs where PBR is configured. This problem is resolved in Release 12.1(5c)E8. (CSCdt35971)
- PBR traffic from WAN interfaces is not Layer 3 switched in hardware. This problem is resolved in Release 12.1(5c)E8. (CSCdt19985)

- Cisco Security Advisory:
  Cisco IOS Software Multiple SNMP Community String Vulnerabilities
  Revision 1.0: INTERIM
  For Public Release2001 February 27 20:00 US/Eastern (UTC+0500)

  Summary:

  Multiple Cisco IOS software and Catalyst OS software releases contain several independent but related vulnerabilities involving the unexpected creation and exposure of SNMP community strings. These vulnerabilities can be exploited to permit the unauthorized viewing or modification of affected devices.

  To remove the vulnerabilities, Cisco is offering free software upgrades for all affected platforms. The defects are documented in DDTS records CSCds32217, CSCds16384, CSCds19674, CSCdr59314, CSCdr61016, and CSCds49183.

  In addition to specific workarounds for each vulnerability, affected systems can be protected by preventing SNMP access.

  This notice will be posted at:

  http://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtml.

  (CSCdr59314, CSCdr61016, CSCds32217)

- Cisco Security Advisory:
  Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability
  Revision 1.0: INTERIM
  For Public Release 2001 February 27 04:00 US/Eastern (UTC+0500)

  Summary:

  Cisco IOS software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB-II system group, such as “sysContact,” “sysLocation,” and “sysName,” that do not affect the device’s normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN-EMULATION-CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial-of-service attack if it is not protected against unauthorized use of the ILMI community string.

  The vulnerability is only present in certain combinations of Cisco IOS releases on Cisco routers and switches. ILMI is a necessary component for ATM, and the vulnerability is present in every Cisco IOS Release that contains the supporting software for ATM and ILMI without regard to the actual presence of an ATM interface or the physical ability of the device to support an ATM connection.

  To remove this vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is documented in DDTS record CSCdp11863.

  In lieu of a software upgrade, a workaround can be applied to certain Cisco IOS releases by disabling the ILMI community or “*ilmi” view and applying an access list to prevent unauthorized access to SNMP. Any affected system, regardless of software release, may be protected by filtering SNMP traffic at a network perimeter or on individual devices.

  This notice will be posted at:

  http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml

  (CSCdp11863)

- A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

  The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the Extended Length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

  The AS_PATH (type code 2) is represented by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems in the segment. The path segment value contains the list of autonomous systems (each AS is represented by two octets).

  The total length of the attribute depends on the number of path segments and the number of autonomous systems in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of autonomous systems (without having to use the extended length bit) is 126 [= (255-2)/2]. If the UPDATE is propagated across an AS boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

  The caveat was caused by the mishandling of the operation during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its iBGP peers would detect the mismatch and issue a NOTIFICATION message (update malformed) to reset their session.

  The average maximum AS_PATH length in the Internet is between 15 and 20 autonomous systems, so there is no need to use the extended length. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

  [Part of the text was taken from RFC 1771.] This problem is resolved in Release 12.1(3a)E3. (CSCdr54230)

- When BGP sessions get reset, currently, with lob neighbor-changes, the event is errlogged. However, to find out the reasons as to why there was a reset, one has to turn on the debugs. This fix will automatically errlog the NOTIFICATION message when the sessions are reset. This feature will be turned on by the same log neighbor-changes knob. (CSCdr54231)

Resolved Caveats in Release 12.1(5a)E3

Note Release 12.1(5a)E3 contains the Service Provider feature set image for Supervisor Engine 1 with MSFC2 (c6sup12-psv-mz.121-5.E3).

- MBGP peer updates with extended attributes are a byte longer than updates without extended attributes. The extra byte overwrites the next-hop data in the update, resulting in malformed updates. This problem is resolved in Release 12.1(5a)E3. (CSCdt06780)

Resolved Caveats in Release 12.1(5a)E1

None.

Resolved Caveats in Release 12.1(5a)E

- Support for mobile IP was inadvertently deleted. This problem is resolved in Release 12.1(5a)E1. (CSCds78103)
- Clock synchronization between the MSFC and the supervisor engine on the Catalyst 6500 series switches is broken and affects other subsystems. This problem is resolved in Release 12.1(5a)E. (CSCds72622)
- The input and output fields of NDE version 7 records are not updated with the snmp_if_index of the ingress and egress interfaces. This problem is resolved in Release 12.1(5a)E. (CSCds39850)

Note Regarding the resolution of CSCds39850, the index stored for the input interface is that of the candidate packet that created the shortcut. Other flows with a similar flow specification that enter the switch on other interfaces can take the same shortcut, but the probability of this can be reduced if you use a more granular flow mask (source-destination or full-flow).

FlexWAN Module Caveats

- Open FlexWAN Module Caveats in Release 12.1(5c)E12, page 312
- Resolved FlexWAN Module Caveats in Release 12.1(5c)E10, page 313
- Resolved FlexWAN Module Caveats in Release 12.1(5c)E9, page 313
- Resolved FlexWAN Module Caveats in Release 12.1(5c)E8, page 313
- Resolved FlexWAN Module Caveats in Release 12.1(5a)E3, page 313

Open FlexWAN Module Caveats in Release 12.1(5c)E12

- When converting from Catalyst software to Cisco IOS on both the supervisor engine and MSFC, the **show interfaces** command for the FlexWAN module might display "administratively down, line protocol is down."

  Workaround: Enter the **shutdown** and **no shutdown** commands for the affected interfaces. This problem is resolved in Release 12.1(6)E. (CSCds86384)
- Flows between an Ethernet interface configured with an HSRP standby IP address and a WAN interface might not be Layer 3 switched. This problem is resolved in Release 12.1(8a)E. (CSCds66364)
- FlexWAN module crashinfo files do not propagate to the MSFC bootflash device.

  Workaround: Display the FlexWAN module crashinfo filename with the **dir cwan***slot_number/port_adapter_number*-**bootflash:** command. You can copy a FlexWAN module **crashinfo** file with the **copy cwan***slot_number/port_adapter_number*-**bootflash:** command. This problem is resolved in Release 12.1(14)E. (CSCdr71603)
- If you enable and disable MMLS on ATM subinterfaces with a combination of point-to-point and multipoint subinterfaces, multicast shortcuts may not be created for multipoint connections, or in some cases multicast traffic may fail. (CSCdr01409)

Note CSCdr01409 is not seen in later releases.

- To use the interfaces on the FlexWAN module, you must enable IP routing on the MSFC. (CSCdp34896)
- With an MSFC2, to avoid error-caused reloads, enter the **no vines route-cache** interface commands so that VINES traffic is process switched. (CSCdr61424)

Note CSCdr61424 is not seen in later releases.

Resolved FlexWAN Module Caveats in Release 12.1(5c)E12

None.

Resolved FlexWAN Module Caveats in Release 12.1(5c)E10

None.

Resolved FlexWAN Module Caveats in Release 12.1(5c)E9

None.

Resolved FlexWAN Module Caveats in Release 12.1(5c)E8

None.

Resolved FlexWAN Module Caveats in Release 12.1(5a)E3

None.

Release 12.1(4)E1

- Open Caveats in Release 12.1(4)E1, page 313
- Resolved Caveats in Release 12.1(4)E1, page 314

Open Caveats in Release 12.1(4)E1

- Support for Mobile IP was inadvertently deleted. This problem is resolved in Release 12.1(5a)E1. (CSCds78103)
- You cannot configure the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr62024, CSCdr54103)
- The **copy running-config startup-config** command does not save the **boot system flash** command in the startup configuration file. Use the **write memory** command instead. This problem is resolved in Release 12.1(6)E. (CSCds43994)
- There is no warning message displayed if you exceed the maximum number (63) of microflow policers. The extra policers are displayed by the **show mls qos ip** command, but they do not work. If classes are increased beyond the maximum number (255) in a policy-map, the policy is rejected without a warning message if applied to an interface. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(6)E. (CSCds38349)

- The IPX **rip-response-delay** interface command does not work on an MSFC, which prevents configuration of preferred routes with this command. (CSCdr45398)

  Note This problem has not been seen in later releases.

- The MSFC2 does not support the MultiNode Load Balancing (MNLB) forwarding agent of the MNLB feature set for LocalDirector. This problem is resolved in Release 12.1(8a)E. (CSCdr65433)
- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) timestamp for the Flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor engine or a PCMCIA card from slave-slot0:when the applications are performing Flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- Downloading images to an Intel Value series 200 Flash card in the PCMCIA slot may in rare situations fail to write a valid image. Downloading during periods of low system activity reduces the likelihood of this failure. This problem is resolved in Release 12.1(6)E (see the related Release 12.0(7)XE1 resolved CSCdm52806 caveat). (CSCdm52806)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)

Resolved Caveats in Release 12.1(4)E1

- After you enter the **no mls qos flow-policing** and **mls qos flow-policing** commands, any microflow policing previously configured on interfaces is not restored. To recover, either remove the service policies that have microflow policing and then reapply them, or enter the **shutdown** command and then the **no shutdown** command on the interfaces. This problem is resolved in Release 12.1(4)E1. (CSCds41316)
- For 48-port 10/100TX RJ-45 Ethernet switching modules (WS-X6248-RJ-45), the output from the **show queueing interface** command does not contain the “Packets dropped on Transmit” section or the “Packets dropped on Receive” section. This problem is resolved in Release 12.1(4)E1. (CSCds39365)
- When an interface configured as a switch port has both an IGMP receiver and a multicast-capable router attached to it, IGMP snooping incorrectly marks the port as only a multicast router port, which disrupts traffic to the multicast receiver if the multicast router attached to the interface goes down. This disruption lasts until IGMP snooping learns the port correctly. In the worst case, the disruption lasts for the IGMP query interval. This problem is resolved in Release 12.1(4)E1. (CSCds54124)
- For a multicast source directly connected to a router, the “R” flag may get set when receiving an (S,G,R) prune if the (S,G) O-list is NULL, and the prune is received on the non-incoming interface (nonIIF). This situation causes the IIF to change to the route processor (RP), and causes the IIF to no longer be the rendezvous point (RP) directly connected to the source, which resets the “F” flag. The RP then loses the (S,G) state and new receivers cannot join the multicast source. This problem is resolved in Release 12.1(4)E1. (CSCds23901)

- Receipt of a large packet that was fragmented by another network device might cause this message to be displayed at the rendezvous point of a multicast network that is running Protocol Independent Multicast (PIM) sparse mode:

  ```
  %PIM-5-REG_ENCAP_INVALID:Bad register from IP_address for (IP_address,
  Class_D_IP_address). Trace = ....
  ```

  This problem is resolved in Release 12.1(4)E1. (CSCdr49641)
- Configuring the source VLAN and filter VLAN of the monitor (SPAN) feature can result in a heap corruption fault and crash. This problem is resolved in Release 12.1(4)E1. (CSCds56632)
- To avoid a fatal exception, do not configure a VLAN as both a monitor session source VLAN and a filter VLAN. This problem is resolved in Release 12.1(4)E1. (CSCds63640)
- With OSPF configured, to avoid multiple MSFCs in the same subnet claiming to be the designated router, use the loopback interface IP address for each router instead of the interface IP address. This problem is resolved in Release 12.1(4)E1. (CSCdr08174, CSCds00527)

Release 12.1(3a)E Rebuilds

- Open Caveats in Release 12.1(3a)E7, page 315
- Resolved Caveats in Release 12.1(3a)E7, page 316
- Resolved Caveats in Release 12.1(3a)E4, page 316
- Resolved Caveats in Release 12.1(3a)E3, page 316

Open Caveats in Release 12.1(3a)E7

- Support for Mobile IP was inadvertently deleted. This problem is resolved in Release 12.1(5a)E1. (CSCds78103)
- You cannot configure the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr62024)
- The **copy running-config startup-config** command does not save the **boot system flash** command in the startup configuration file. Use the **write memory** command instead. This problem is resolved in Release 12.1(6)E. (CSCds43994)
- You cannot set the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr54103)
- For 48 Port 10/100TX RJ-45 Ethernet switching modules (WS-X6248-RJ-45), the output from the **show queueing interface** command does not contain the **Packets dropped on Transmit** section or the **Packets dropped on Receive** section. This problem is resolved in Release 12.1(4)E1. (CSCds39365)
- There is no warning message displayed if you exceed the maximum number (63) of microflow policers. The extra policers are displayed by the show mls qos ip command, but they do not work. If classes are increased beyond the maximum number (255) in a policy-map, the policy is rejected without a warning message if applied to an interface. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(6)E. (CSCds38349)

- The MSFC2 does not support the MultiNode Load Balancing (MNLB) forwarding agent of the MNLD feature set for Local Director. This problem is resolved in Release 12.1(8a)E. (CSCdr65433)
- To avoid multiple MSFCs in the same subnet claiming to be the OSPF designated router, use the loopback interface IP address for each router rather than the interface IP address. This problem is resolved in Release 12.1(4)E1. (CSCdr08174, CSCds00527)
- After you enter the **no mls qos flow-policing** and **mls qos flow-policing** commands, any microflow policing previously configured on interfaces is not restored. To recover, either remove the service policies that have microflow policing and then reapply them, or enter **shutdown** and then **no shutdown** commands on the interfaces. This problem is resolved in Release 12.1(4)E1. (CSCds41316)
- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) timestamp for the Flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor engine or a PCMCIA card from slave-slot0:when the applications are performing Flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- Downloading images to an Intel Value series 200 Flash card in the PCMCIA slot may in rare situations fail to write a valid image. Downloading during periods of low system activity reduces the likelihood of this failure. This problem is resolved in Release 12.1(6)E (see the related Release 12.0(7)XE1 resolved CSCdm52806 caveat). (CSCdm52806)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)

Resolved Caveats in Release 12.1(3a)E7

- An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  This problem is resolved in Release 12.1(3a)E7. (CSCdw65903)

Resolved Caveats in Release 12.1(3a)E4

- Caveat CSCdr91706 is resolved in Release 12.1(3a)E4.

Resolved Caveats in Release 12.1(3a)E3

- A spurious access may occur when the **bgp deterministic med** command is configured. This problem is resolved in Release 12.1(3a)E3. (CSCdr43297)
- The switch might display a HEARTBEAT-SP-6-NOT_HEARD message and reload. This problem is resolved in Release 12.1(3a)E3. (CSCdr97710)
- PIM sparse mode for the Auto-RP groups might not set the “L” flag for the 224.0.1.40 RP-discovery group. This problem is resolved in Release 12.1(3a)E3. (CSCdr51872)
- In a redundant configuration, there is no command that identifies the active supervisor engine. As a workaround, enter the **show idprom sup 1** and **show idprom sup 2** commands. The command that fails identifies the redundant supervisor engine. This problem is resolved in Release 12.1(3a)E3 with the **show module** command. (CSCdr29969)

- CLNS fast-switching does not work. This problem is resolved in Release 12.1(3a)E3. (CSCdr17019)
- The ifInNUcastPkts MIB object (1.3.6.1.2.1.2.2.1.12) does not increment correctly. This problem is resolved in Release 12.1(3a)E3. (CSCds07072)

Release 12.1(2)E and Rebuilds

- Open Caveats in Release 12.1(2)E2, page 317
- Resolved Caveats in Release 12.1(2)E2, page 317
- Resolved Caveats in Release 12.1(2)E, page 318

Open Caveats in Release 12.1(2)E2

- You cannot configure the MTU size on VLAN interfaces. For Supervisor Engine 2, this problem is resolved in Release 12.1(8a)E. For Supervisor Engine 1, this problem is resolved in Release 12.1(7)E. (CSCdr62024)
- The **copy running-config startup-config** command does not save the **boot system flash** command in the startup configuration file. Use the **write memory** command instead. This problem is resolved in Release 12.1(6)E. (CSCds43994)
- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) timestamp for the flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor or a PCMCIA card from slave-slot0:when the applications are performing flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- Downloading images to an Intel Value series 200 flash card in the PCMCIA slot may in rare situations fail to write a valid image. Downloading during periods of low system activity reduces the likelihood of this failure. This problem is resolved in Release 12.1(6)E (see the related Release 12.0(7)XE1 resolved CSCdm52806 caveat). (CSCdm52806)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)
- In a redundant configuration, there is no command that identifies the active supervisor engine. As a workaround, enter **show idprom sup 1** and **show idprom sup 2** commands. The command that fails identifies the redundant supervisor engine. This problem is resolved in Release 12.1(3a)E3 with the show module command. (CSCdr29969)

Resolved Caveats in Release 12.1(2)E2

- An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  This problem is resolved in Release 12.1(2)E2. (CSCdw65903)

Resolved Caveats in Release 12.1(2)E

- BOOTP/DHCP address request UDP packets are dropped because of an encapsulation failure. This problem is resolved in Release 12.1(2)E. (CSCdp36754)
- DLSw Ethernet redundancy is not supported. This problem is resolved in Release 12.1(2)E. (CSCdp93599)
- Online insertion or replacement of a secondary supervisor engine can cause the Gigabit Ethernet ports on the secondary supervisor engine to be unusable for approximately 5 minutes. This problem is resolved in Release 12.1(2)E. (CSCdp95029)

Release 12.1(1)E and Rebuilds

- Open Caveats in Release 12.1(1)E6, page 318
- Resolved Caveats in Release 12.1(1)E6, page 318
- Resolved Caveats in Release 12.1(1)E2, page 319
- Resolved Caveats in Release 12.1(1)E, page 319

Open Caveats in Release 12.1(1)E6

- The **copy running-config startup-config** command does not save the **boot system flash** command in the startup configuration file. Use the **write memory** command instead. This problem is resolved in Release 12.1(6)E. (CSCds43994)
- DLSw Ethernet redundancy is not supported. This problem is resolved in Release 12.1(2)E. (CSCdp93599)
- The ciscoFlashDeviceInitTime CISCO-FLASH-MIB object does not return the correct device initialization (insertion or removal) timestamp for the flash devices on a redundant supervisor engine. Users of applications that depend on ciscoFlashDeviceInitTime should take care not to remove a redundant supervisor or a PCMCIA card from slave-slot0:when the applications are performing flash file operations. This problem is resolved in Release 12.1(11b)E. (CSCdp98597)
- Online insertion or replacement of a secondary supervisor engine can cause the Gigabit Ethernet ports on the secondary supervisor engine to be unusable for approximately 5 minutes. This problem is resolved in Release 12.1(2)E. (CSCdp95029)
- Downloading images to an Intel Value series 200 flash card in the PCMCIA slot may in rare situations fail to write a valid image. Downloading during periods of low system activity reduces the likelihood of this failure. This problem is resolved in Release 12.1(6)E (see the related Release 12.0(7)XE1 resolved CSCdm52806 caveat). (CSCdm52806)
- A traceback message displays when you exit the switch console. This message is harmless and can be safely ignored. This problem is resolved in Release 12.1(8a)E. (CSCdp35517)

Resolved Caveats in Release 12.1(1)E6

- An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  This problem is resolved in Release 12.1(1)E6. (CSCdw65903)

Resolved Caveats in Release 12.1(1)E2

- After setting the config-register to 0x02, entering a sync command, and reloading, the config-register is 0x0. This problem is resolved in Release 12.1(1)E2. (CSCdr25147)
- The SLB stateless redundancy **inservice standby** *name* command results in an endless loop. This problem is resolved in Release 12.1(1)E2. (CSCdr24308)
- If the egress interface list for a multicast flow is empty (because there are no interested hosts or multicast routers), the multicast flow may not get Layer 3 switched. A high volume of traffic to the empty egress interface list can cause high MSFC CPU utilization.

  Workaround: Enter the **show ip mroute** command to identify flows that are not Layer 3 switched and then enter the **clear ip mroute** command for the identified multicast flows. This problem is resolved in Release 12.1(1)E2. (CSCdr22769)
- Following a reload, SLB does not load-balance traffic until the **shutdown** and then the **no shutdown** commands are entered for the SLB interfaces. This problem is resolved in Release 12.1(1)E2. (CSCdp95180)
- With CEF enabled on an MSFC that is serving as the active HSRP router, pinging across the MSFC has only a 50-percent success rate. This problem is resolved in Release 12.1(1)E2. (CSCdm68596)
- On an MSFC with CEF enabled, IP traffic through tunnel interfaces experiences packet loss. This problem is resolved in Release 12.1(1)E2. (CSCdr16213)
- The MLS entry for an end station must be manually cleared if, before the MLS entry ages out, the end station is replaced by another that uses the same IP address but that has a different MAC address. This problem is resolved in Release 12.1(1)E2. (CSCdp64112)
- WCCP does not work with CEF enabled. This problem is resolved in Release 12.1(1)E2. (CSCdr10156)
- On the WS-X6408-GBIC 8-port Gigabit Ethernet switching module, when QoS is enabled:
  - It is safe to ignore “port_rx_enable errors” messages displayed following the **no shutdown** command or reload.
  - QoS WRR configuration commands for WS-X6408-GBIC ports are not saved in NVRAM. You must manually reenter any nondefault QoS WRR configuration commands for WS-X6408-GBIC ports after reboot.
  - Gigabit EtherChannels can contain ports on one or more WS-X6408-GBIC switching modules. Gigabit EtherChannels that contain ports on a WS-X6408-GBIC switching module and on a WS-X6K-SUP1-2GE supervisor engine fail.

  This problem is resolved in Release 12.1(1)E2. (CSCdp81930)

Resolved Caveats in Release 12.1(1)E

- Power cycling the redundant supervisor engine is not supported. This problem is resolved in Release 12.1(1)E. (CSCdp55523)
- An error-caused reload does not write a crashinfo file for the MSFC. This problem is resolved in Release 12.1(1)E. (CSCdp94153)
- In a switch with redundant supervisor engines, the slot0 device and the MSFC bootflash device on the redundant supervisor engine are accessible. The bootflash device on the redundant supervisor engine is not accessible. Because converting from Catalyst software to Cisco IOS software requires formatting the supervisor engine bootflash device, do not convert switches while redundant

supervisor engines are installed. With the switch in a nonredundant configuration, do the conversion separately for each supervisor engine, and then configure redundancy. This problem is resolved in Release 12.1(1)E. (CSCdp55717)

- Partial support exists for the CISCO-FLASH-MIB. This problem is resolved in Release 12.1(1)E.
- Partial support exists for the BRIDGE-MIB (RFC 1493). This problem is resolved in Release 12.1(1)E. (CSCdm44194)
- Partial support exists for the CISCO-STP-EXTENSIONS-MIB. This problem is resolved in Release 12.1(1)E. (CSCdp50869)

Troubleshooting

These sections describes troubleshooting guidelines for the Catalyst 6500 series switch configuration:

- Recovering From Loss of the Boot Loader Image, page 320
- System Troubleshooting, page 320
- Module Troubleshooting, page 321
- VLAN Troubleshooting, page 321
- Spanning Tree Troubleshooting, page 321
- Additional Troubleshooting Information, page 323



Note To attempt recovery from MSFC ROMMON, enter the **confreg 0x2102** and **reset** ROMMON commands.

Recovering From Loss of the Boot Loader Image

If you lose the boot loader image, refer to this online publication for boot loader image recovery procedures:

http://www.cisco.com/warp/customer/473/14.html

System Troubleshooting

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- After you initiate a switchover from the active supervisor engine to the redundant supervisor engine, or when you insert a redundant supervisor engine in an operating switch, always wait until the supervisor engines have synchronized and all modules are online before you remove or insert modules or supervisor engines or perform another switchover.
- If you have an interface whose speed is set to **auto** connected to another interface whose speed is set to a fixed value, configure the interface whose speed is set to a fixed value for half duplex. Alternately, you can configure both interfaces to a fixed-value speed and full duplex.

Module Troubleshooting

This section contains troubleshooting guidelines for module problems:

- When you hot insert a module into a chassis, be sure to use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 6500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, make sure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

VLAN Troubleshooting

Note Catalyst 6500 series switches do not support ISL-encapsulated Token Ring frames. To support trunked Token Ring traffic in your network, make trunk connections directly between switches that support ISL-encapsulated Token Ring frames. When a Catalyst 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a switch acting on these forwarded DTP frames, do the following:

- For interfaces connected to devices that do not support DTP, in which trunking is not currently being used, configure interfaces with the **switchport mode access** command, which puts the interface into access mode and sends no DTP frames.
- When manually enabling trunking on a link to devices that do not support DTP, use the **switchport nonegotiate** and **switchport mode trunk** commands, which puts the interface into trunking mode without sending DTP frames.

Spanning Tree Troubleshooting

The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, switches receive spanning tree bridge protocol data units (BPDUs) periodically from neighboring switches. You can configure the frequency with which BPDUs are received by entering the **spanning-tree vlan** *vlan_ID* **hello-time** command (the default frequency is set to 2 seconds). If a switch does not receive a BPDU in the time period defined by the **spanning-tree vlan** *vlan_ID* **max-age** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the switch waits for the time period specified by the **spanning-tree vlan** *vlan_ID* **forward-time** command (15 seconds by default) in each of these intermediate states. If a blocked spanning tree interface does not receive BPDUs from its neighbor within 50 seconds, it moves into the forwarding state.

Note We do not recommend using the UplinkFast feature on switches with more than 20 active VLANs. The convergence time might be unacceptably long with more than 20 active VLANs.

To debug STP problems, follow these guidelines:

- The sum of all logical interfaces equals the number of trunks on the switch times the number of active VLANs on the trunks, plus the number of nontrunking interfaces on the switch.
- The **show spanning-tree summary totals** command displays the number of logical interfaces in the STP Active column.
- These maximum numbers of logical interfaces are supported with Release 12.1(13) E and later releases:

	MST	RPVST+	PVST+
Supervisor Engine 2, MSFC2	50,000 total 6,000[1] per switching module	10,000 total 1,800[1] per switching module	13,000 total 1,800[1] per switching module
Supervisor Engine 1, MSFC or MSFC2	25,000 total 3,000[1] per switching module	6,000 total 1,200 per switching module	6,000 total 1,200 per switching module

1. 10 Mbps, 10/100 Mbps, and 100 Mbps switching modules support a maximum of 1,200 logical interfaces per module.

- These maximum numbers of logical interfaces are supported with 12.1 E releases earlier than Release 12.1(13)E:

	PVST+
Supervisor Engine 2, MSFC2	4,500 total 1,800[1] per switching module
Supervisor Engine 1, MSFC or MSFC2	4,500 total 1,200 per switching module

1. 10 Mbps, 10/100 Mbps, and 100 Mbps switching modules support a maximum of 1,200 logical interfaces per module.

Note Cisco IOS software displays a message if you exceed the maximum number of logical interfaces.

- After a switchover from the active to the redundant supervisor engine, the ports on the redundant supervisor engine take longer to come up than other ports.
- Record all spanning tree-blocked ports in each switch in your network. For each of the spanning tree-blocked ports, record the output of the **show interface** command. Check to see if the port has registered many alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs. If the input queue counter is incrementing continuously, the port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.
- On a blocked spanning tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of its neighboring device.

- On trunks, make sure that the trunk configuration is set properly on both sides of the link.
- On trunks, if the neighboring device supports it, set duplex to full on both sides of the link to prevent any collisions under heavy traffic conditions.

Additional Troubleshooting Information

For additional troubleshooting information, refer to the publications at this URL:

http://www.cisco.com/en/US/partner/products/hw/switches/tsd_products_support_category_home.html

System Software Upgrade Instructions

See this publication:

http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_configuration_example09186a0080116ff0.shtml

Converting from Catalyst Software

See these publications:

http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_tech_note09186a00801350b8.shtml

http://www.cisco.com/warp/public/473/81.html

Documentation Updates

This section describes updates to the product documentation. These changes will be included in the next update to the documentation.

Errors

None.

Omissions

None.

Changes

Some printed copies of the *Cisco 7603 and 7606 Internet Router Installation Guide*, *Cisco 7609 Internet Router Installation Guide*, and *Cisco 7600 Internet Router Module Installation Guide* might show support for the 2-port channelized OC-48 OSM (OSM-2CHOC48/T3) and the 8-port channelized OC-12 OSM (OSM-8CHOC12/T3), which are no longer available.

Related Documentation

These sections describe the documentation available for Cisco IOS on the supervisor engine and MSFC. These publications consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other publications. Documentation is available as printed manuals or electronic publications.

Use these release notes with these publications:

- Platform-Specific Publications, page 324
- Cisco IOS Software Documentation Set, page 324

Platform-Specific Publications

These publications are available for the Catalyst 6500 series switches running Cisco IOS software on the supervisor engine and MSFC:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/index.htm

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Catalyst 6500 Series Switch Cisco IOS System Message Guide*

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting publications.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. You can use each configuration guide in conjunction with its corresponding command reference. Two master hot-linked publications provide information for the Cisco IOS software documentation set on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm

Release 12.1 Documentation Set

The following table describes the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and orderable in printed form.

Note You can find the most current Cisco IOS documentation on Cisco.com. These electronic publications may contain updates and modifications made after the hard-copy publications were printed.

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume I* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
• *Cisco IOS Dial Services Configuration Guide: Terminal Services* • *Cisco IOS Dial Services Configuration Guide: Network Services* • *Cisco IOS Dial Services Command Reference*	Preparing for Dial Access Modem Configuration and Management ISDN and Signaling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
• *Cisco IOS IP and IP Routing Configuration Guide* • *Cisco IOS IP and IP Routing Command Reference*	IP Addressing and Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX

Books	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
• *Cisco IOS Multiservice Applications Configuration Guide* • *Cisco IOS Multiservice Applications Command Reference*	Multiservice Applications Overview Voice Video Broadband
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping signaling Link Efficiency Mechanisms Quality of Service Solutions
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching MPLS Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
• *New Features in 12.1-Based Limited Lifetime Releases* • *New Features in Release 12.1 T* • Release Notes (release note and caveat documentation for 12.1-based releases and various platforms) • *Cisco IOS Debug Command Reference* • *Cisco IOS Dial Services Quick Configuration Guide*	

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the *Catalyst 6500 Series IOS Software Configuration Guide* and the *Catalyst 6500 Series IOS Command Reference* publications.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 1999–2007 Cisco Systems, Inc. All rights reserved.
